Command, Control, Communications, and Computers (C4).

1. INTRODUCTION

1.0 PURPOSE. The purpose of the Command, Control, Communications, and Computers (C4) area is to (1) review the technical descriptions of the systems associated with the C4 functions; (2) review the threats to C4 systems' survivability; (3) assess the susceptibility and vulnerability to those threats; (4) present promising survivability enhancement features; and (5) assess system survivability status in the near (FY01-02), mid (FY03-08), and far terms (FY9-16). This section provides an understanding of current/future C4 systems and the associated threats, but is primarily intended for three categories of personnel: (1) requirements developers (e.g., Battle Labs, Directorates of Combat Development) who focus experimentation and requirements documentation on survivability shortfalls, (2) materiel developers (e.g., Program Executive Offices; Program, Project, and Product Managers; Research, Development, and Engineering Centers) who can enhance survivability through systems design and upgrades, and (3) science and technology planners and researchers who explore and develop broad-based survivability technologies.

1.1 DEFINITIONS.

1.1.1 **Survivability**. Survivability is defined in the Department of Defense (DoD) Regulation 5000.2, *Mandatory Procedures for Major Defense Acquisition Programs (MDAPS) and Major Automated Information System (MAIS) Acquisition Programs,* 15 March 1996 as "the capability of a system and crew to avoid or withstand a manmade hostile environment without suffering an abortive impairment of its ability to accomplish its designated mission." There are two types of system survivability: physical and operational. Physical survivability is the capability of a system (including its operators) to avoid or resist measures taken by the enemy to destroy it. Operational survivability is the capability of a system to avoid or resist measures taken by the enemy to cause an interruption of mission performance (i.e., destruction, interference, data manipulation, deception, etc.). If the risk from attacks against C4 assets cannot be completely avoided, survivability is still achieved if the threat can be successfully managed. The Army Research Laboratory's (ARL) Survivability/Lethality Analysis Directorate (SLAD) provides value-added technical data, sound analysis and affordable recommendations regarding survivability throughout a system's life cycle from requirements formulation through system design, test and evaluation, materiel fielding, and product improvement. Through modeling, experiments, and analyses, SLAD characterizes the survivability of weapon systems and the individual soldier to the full spectrum of threats.

1.1.2 **Soldier Survivability**. The roles and responsibilities for soldier survivability are outlined in the Army's survivability regulation, Army Regulation (AR) 70-75 and AR 602-2, *Manpower and Personnel Integration (MANPRINT) in the System Acquisition Process.* These regulations define soldier survivability in both system and soldier terms, as follows: SYSTEM – The characteristics that can reduce fratricide, as well as reduce detectability of the soldier, prevent attack if detected, prevent damage if attacked, minimize medical injury if wounded or otherwise injured, and reduce physical and mental fatigue; and SOLDIER – Those characteristics that enable soldiers to withstand (or avoid) adverse military actions or the effects of the natural phenomena that would result in the loss of capability to continue effective performance of the prescribed mission.

1.1.3 **Susceptibility and Vulnerability.** The key words in the DoD Regulation 5000.2 survivability definition are “to avoid or withstand.” These terms are measures of a system’s susceptibility and vulnerability to the hostile environment.

1.1.3.1 Susceptibility. Susceptibility, as used in this document, is the degree to which a device, equipment, or weapon system is open to effective attack due to one or more inherent weaknesses. Susceptibility can be divided into three general categories of threat activity: (1) detecting, identifying, acquiring, and tracking; (2) missile launch, gun firing, or the initiation of other forms of attack (e.g., computer network attack) intended to disrupt or destroy equipment, data, and/or system capabilities; and (3) impact or detonation of warheads or other “munitions” (e.g., viruses, electromagnetic energy, database corruption/manipulation, etc.) intended to disrupt or destroy equipment and/or system capabilities. System susceptibility is influenced by such features as the system design (e.g., signature and maneuverability), tactics used (e.g., terrain masking to avoid detection), and survivability equipment/weapons it carries (e.g., electronic attack (EA) measures to avoid smart munitions or firewalls).

1.1.3.2 Vulnerability. Vulnerability, as used in this document, is the characteristic of a system that causes it to suffer a definite degradation (loss or reduction of capability to perform a designated mission) as a result of having been subjected to a certain (defined) level of effects in a manmade hostile environment. To properly identify system vulnerabilities, there must be a determination of the survivability features imbedded in the system's design and any added features that reduce the effects of damage when the system is in a hostile environment. Vulnerability is influenced by such things as the ability to continue to operate after a hit/data intrusion, as well as system design features and equipment that prevent or suppress damage to critical components or databases.

1.2 PHYSICAL SURVIVABILITY AVOIDANCE CATEGORIES. In general, the physical survivability of C4 systems is largely dependent upon the characteristics of those platforms upon which they are mounted or installed. Because the physical survivability of these platforms is discussed in detail in other subject areas, physical survivability of C4 systems is only briefly discussed here. The Army’s strategy for increasing physical survivability of C4 systems, as shown in Figure 1.2-1, is primarily based on avoidance.

- Avoid being detected.
- If detected, avoid being acquired as a target.
- If acquired as a target, avoid being hit.
- If hit, avoid penetration/system intrusion.
- If penetrated, avoid being killed.

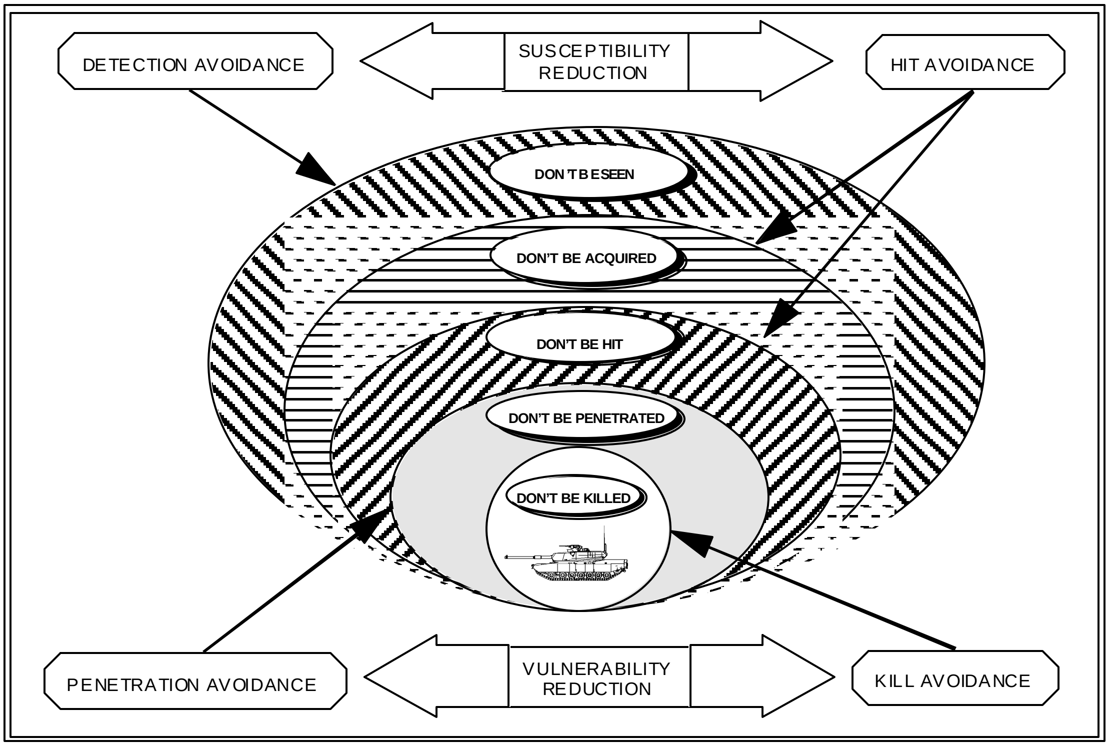


Figure 1.2-1. Threat Avoidance Categories

As shown in Figure 1.2-1, system survivability technologies being developed can be grouped into four separate categories. These categories are detection avoidance, hit avoidance, penetration avoidance, and kill avoidance.

1.2.1 **Detection Avoidance.** Detection avoidance includes technologies and methods used to suppress the sights, sounds, and images naturally associated with systems.

1.2.2 **Hit Avoidance.** Hit avoidance refers to technologies that reduce the probability of being hit by a weapon after being detected by the enemy.

1.2.3 **Penetration Avoidance.** After being detected, acquired, and hit, a system must be capable of minimizing and/or preventing penetration in order to survive.

1.2.4 **Kill Avoidance.** After being detected, acquired, hit, and penetrated, a C4 system and its crew can survive with the help of kill avoidance technologies.

1.3 OPERATIONAL SURVIVABILITY CATEGORIES. While physical survivability presents a significant threat to Army C4 systems' survivability, the greatest potential threats are in the area of information operations (IO) attack. The Army's intent is to field a digitization capability with a level of information systems protection sufficient to allow critical functions and operations to continue. The Army:

- knows there are vulnerabilities associated with digitized systems;
- is serious about protecting against these vulnerabilities;

- recognizes that complete protection against all known and future vulnerabilities is not possible;

- believes protection, including resiliency and recoverability, must be engineered into the systems, and particularly system of systems, rather than addressed after the fact; and

- recognizes that the desired level of protection is achieved through a comprehensive program of doctrine, training, leadership, and organization, as well as material solutions.

Information systems protection that is sufficient to allow critical functions and operations to continue during and after an IO attack is incorporated into the following operational survivability categories:

- protect,

- detect, and

- restore.

Integrating technologies that support the three C4 system operational survivability categories provides the greatest opportunity of ensuring data availability, integrity, authentication, confidentially, and nonrepudiation.

1.3.1 **Protect.** "Protect" refers to technologies that are capable of minimizing and/or preventing penetration of the C4 system. Protect for operational survivability is similar to the penetration avoidance of physical survivability. Information systems protection should be built into the architecture and design of systems, networks, and the overall infrastructure; implemented concurrent with the implementation of the components of the digitization architecture; and assessed throughout the development process. Protection from computer network attacks (CNAs) requires C2 Protect measures to protect the structural integrity of the network and databases. An example of a type of protection for information systems against unauthorized intrusions is a "firewall." A firewall is an electronic device that is built "around" a network to protect it from the outside. Firewalls enforce the security policy of the network. A given firewall may be designed to protect a poorly secured network from outside threats or to protect a highly secure network from a larger, less secure one. The type of firewall required to protect a system from penetration requires analyzing the threat and defining the level of risk. Protection can be supported by specific components, such as firewalls and guards, as well as by features that are inherent in the design of the information system.

1.3.2 **Detect.** Despite systems that are designed with security in mind, appropriate procedures, and highly skilled personnel, the Army cannot "bullet-proof" digitization infrastructure. Consequently, it is necessary to maintain the ability to do real-time security management and intrusion detection as part of routine operations and to take appropriate reactive measures should an incident occur. The information systems protection concept envisions real-time security management as a component of, and incorporated into, network and system management. Security management must encompass the means to alert the network/system manager to intrusion attempts, as well as a range of response mechanisms. These include the ability to change boundaries/perimeters; reconfigure firewalls, guards, and routers; reroute traffic; change the level of encryption or rekey; remotely “zeroize” communications that are suspected of being compromised; remotely reestablish a net without selected members; and change authentication/passwords and adaptive security measures based on threat level.

1.3.3 **Restore.** Criteria for the digitization system architecture will balance user performance requirements (typically expressed in terms of connectivity, speed of service, or message completion rates) with security-related architecture features such as redundancy, resiliency, and recoverability. Information systems protection should be designed so that damage can be contained and precluded from cascading across the battlefield. If a system is penetrated and the data destroyed, there must be a capability to restore the data.

1.4 SURVIVABILITY ENHANCEMENT OPPORTUNITIES. Survivability analysis consists of the examination of all performance parameters that affect a C4 system’s ability to perform an assigned mission in a manmade hostile environment. Thus, survivability starts with the identification of system susceptibilities and vulnerabilities. Systems survivability is enhanced by technologies that make them harder to detect, acquire, hit, penetrate, and kill. While there is some overlap between the technologies and techniques used to achieve both physical and operational survivability, for the most part, the survivability enhancements discussed here will concentrate on those dealing with the IO attack threat. The physical survivability of future C4 systems relies, to a great extent, on survivability improvements to host systems (e.g., armor, visual camouflage, and site security measures). Additionally, C4 systems are inherently susceptible to detection and acquisition because of their distinctive visual and electromagnetic signatures and unauthorized access through a networked environment. Figure 1.4-1 shows that CNA fall in the penetration avoidance/kill avoidance area as it relates to vulnerability. In the emerging tactical internet (TI), while each of the component systems retains its organic security features, the seamless connectivity achieved generates new vulnerabilities and provides greater opportunity to exploit vulnerabilities, which were always there. The risk from CNAs against Army C4 assets cannot be successfully avoided, but they can be successfully managed. Future systems must address both physical and operational survivability concerns while improving performance. Survivability enhancement options become more expensive the further along a system is in the acquisition process. It is critical that survivability issues are addressed in the early design phase, but it must be assumed that the threat will penetrate some of the time and that soldiers and equipment will be vulnerable. This requires that actions be taken to limit the effects of the penetration.

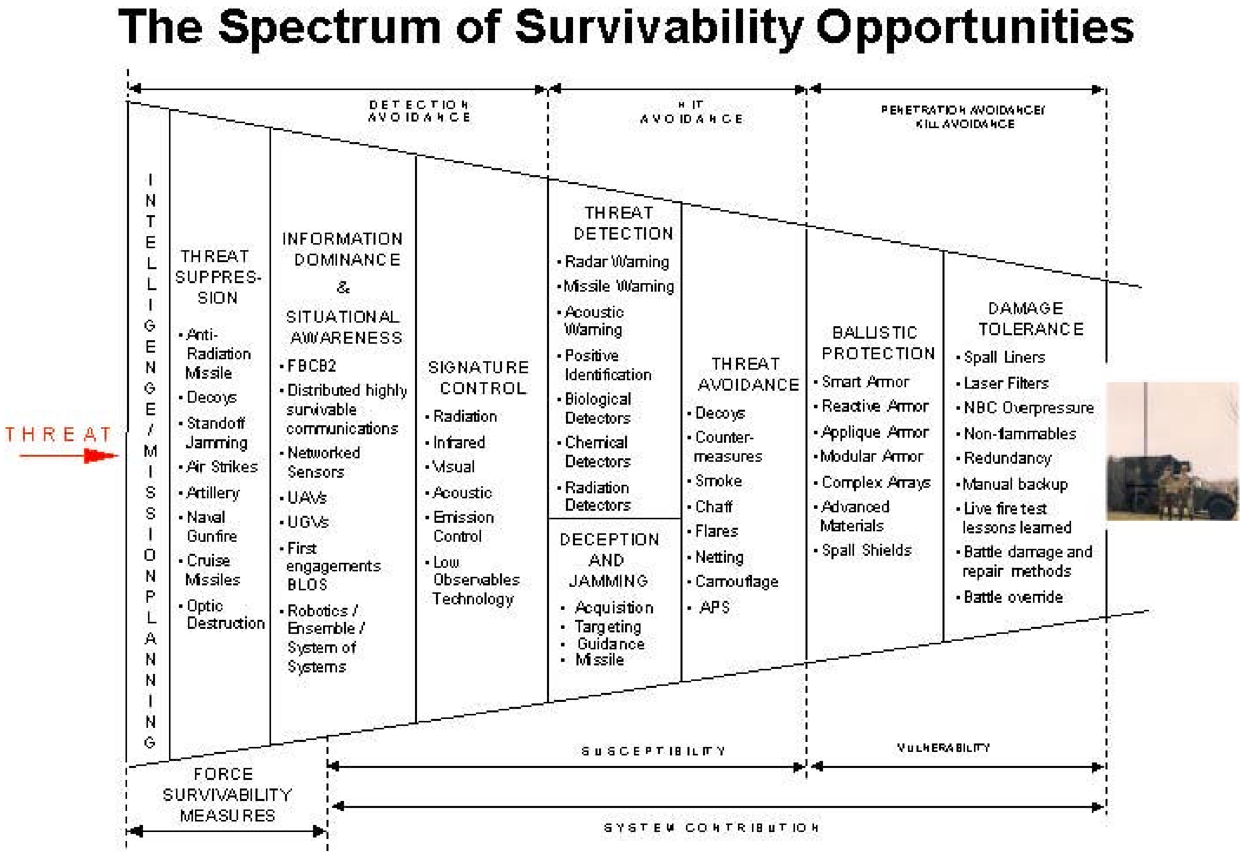


Figure 1. 4-1. Spectrum of Survivability Enhancement Opportunities

1.5 SURVIVABILITY ANALYSIS METHODOLOGY. In order to determine which survivability features increase the effectiveness of a C4 system, a survivability analysis must be conducted to determine the change in the offensive and defensive effectiveness measures. The flow of the analysis task is illustrated in Figure 1.5-1.

1.5.1 **Survivability Analysis Steps.** There are five major steps in the survivability analysis process: threat analysis, survivability requirements, system design/description, susceptibility analysis, and vulnerability/lethality analysis. They are, in fact, very closely related, and, in most cases, involvement in one area requires involvement in one or more of the other areas. The reason they are depicted as part of a pentagon is to emphasize the importance of their interdependence. The end result of the process is information, which results in a more survivable system or knowledge of and acceptance of risk.

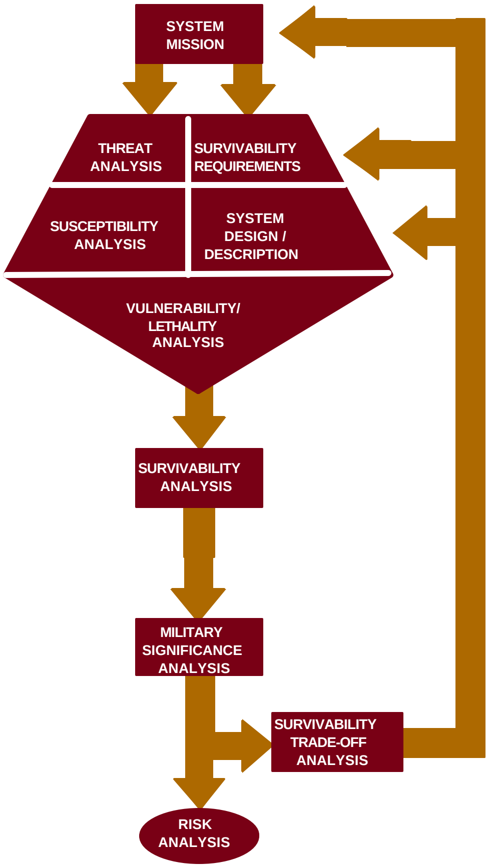

SYSTEM MISSION
THREAT ANALYSIS
SURVIVABILITY REQUIREMENTS
SUSCEPTIBILITY ANALYSIS
SYSTEM DESIGN / DESCRIPTION
VULNERABILITY/ LETHALITY ANALYSIS
SURVIVABILITY ANALYSIS
MILITARY SIGNIFICANCE ANALYSIS
SURVIVABILITY TRADE-OFF ANALYSIS
RISK ANALYSIS

Figure 1.5-1.   Flow of Survivability Analysis Methodology

2. C4 WARFIGHTING CONCEPT

2.0 INTRODUCTION. C4 is the Army's force multiplier for the digitized battlefield of the XXI Century. Synonymous with "information superiority" as defined by the Chairman, Joint Chiefs of Staff, C4 is the capability to collect, process, and disseminate an uninterrupted flow of information while exploiting or denying the adversary's ability to do the same. U.S. Army C4 programs are designed to develop the technologies and architectures needed to provide warfighters the right information, in the right place, at the right time. To accomplish this, the Army requires flexible architectures that permit the following:

- common software for a variety of decisionmaking toolkits;
- modeling and simulation (M&S) technologies that facilitate early assessment of new technologies and warfighting analyses, enhance the ability to "view" systems and immerse humans in the virtual world, and facilitate more effective use of M&S technology for training and mission rehearsal;
- information assurance and distribution among heterogeneous systems;
- seamless communication systems using commercial and common protocols (allowing information transport anywhere in the world); and,
- computing and software technology that supports the evolution of products inserted into common systems.

2.1 C4 FUNCTIONAL AREAS. Decisionmaking and seamless communications (mobile networking, unattended sensors networking, information assurance, antennas and secure personal communication, and reachback), along with computing and software, are the pillars of C4. For analysis purposes, decisionmaking and seamless communications will be the basis for the discussion on threats, vulnerabilities to those threats, survivability enhancement programs, and survivability shortfalls and recommendations.

2.1.1 **Decisionmaking.** Decisionmaking is the heart of the command process and affords the warfighter consistent battlespace understanding, forecasting, planning and resource allocation, and integrated force and execution management. Decisionmaking encompasses development of common, modular components that weave together joint mission planning, rehearsal, execution monitoring, and common pictures of the battlespace. The major emphasis is on acquiring and assimilating information needed to dominate and neutralize adversary forces. A key capability is near-real-time awareness of the location and activity of friendly, enemy, and neutral elements throughout the battlefield area, providing a common awareness of the current situation. A primary objective of information dominance is to meet the warfighters' needs for a flexible command structure that can be rapidly configured and dynamically adapted to optimize force effectiveness and survivability. The warfighter will be provided an intuitive view of the battlespace—an advanced perspective of information and the ability to explore alternative courses of action in faster than real time (e.g., exploring a 10-hour engagement in several minutes).

2.1.2 **Seamless Communications.** Seamless communications connotes assured, user-transparent, secure connectivity among globally dispersed forces—down to the lowest echelon foot soldier, platform, and aircraft. Seamless communications will be accomplished using a combination of U.S. government, foreign government, and commercial infrastructures, as well as military surface and space-based networks operating over a wide range of frequencies. A range of transmission media, bandwidth, standards, and protocols will be automatically accommodated by the networks. Voice and all types of data will be handled within a uniform information transport infrastructure. These technologies will provide the commander high-capacity, flexible, tactical communications to serve all user categories and satisfy the need for reliable communications, irrespective of system limitations, throughout all phases of an operation. In particular, the success of the Army's Future Combat System (FCS) concept is heavily dependent upon the ability to provide an assured networked communications grid. Implementation will be realized via a multitiered communications architecture providing wide-area coverage and allowing an FCS-equipped force to traverse large areas while remaining interconnected; this grid must appear as a homogeneous communications asset to the user. Seamless communications support split-based operations by spanning the globe and interconnecting command echelons, services, and allies worldwide through common transport protocols and dynamic network management. Seamless communications facilitate the warfighters' needs for FCS information, dominance, information warfare, real-time logistics control, and military operations on urbanized terrain (MOUT).   Communications is the mechanism to achieve secure, reliable, timely, and survivable battlefield command and control, as well as information dominance.

2.2 INTEGRATED ARCHITECTURE. When integrated, C4 components and systems provide an architecture that supports the digitized battlefield from the Pentagon to the foxhole. This integrated architecture is depicted pictorially in Figure 2.2-1. The Command and Control (C2) requirements and systems have been pulled together under the Army Battle Command System (ABCS) as shown in Figure 2.2-2. ABCS focuses on the seamless flow of data around the battlefield by placing under one C2 umbrella the Army portion of the Global Command and Control System - Army (GCCS-A), Army Tactical Command and Control System (ATCCS), and the Force XXI Battle Command for Brigade and Below (FBCB2). ABCS reflects the Army's vision for the future battlefield by capitalizing on the power of emerging technology. ABCS takes advantage of broadcast battlefield information, as well as other sources of information, and integrates information, including real-time friendly and enemy situations, into digitized images for display at all levels. This increase in situational awareness forms the essence of a unit's battlespace and provides the basis for the commander's visualization of that battlespace. A shared common picture of the battlefield by commanders at every level will allow precise execution of missions in unison and greatly reduce the fog, confusion, and friction inherent in any operation.

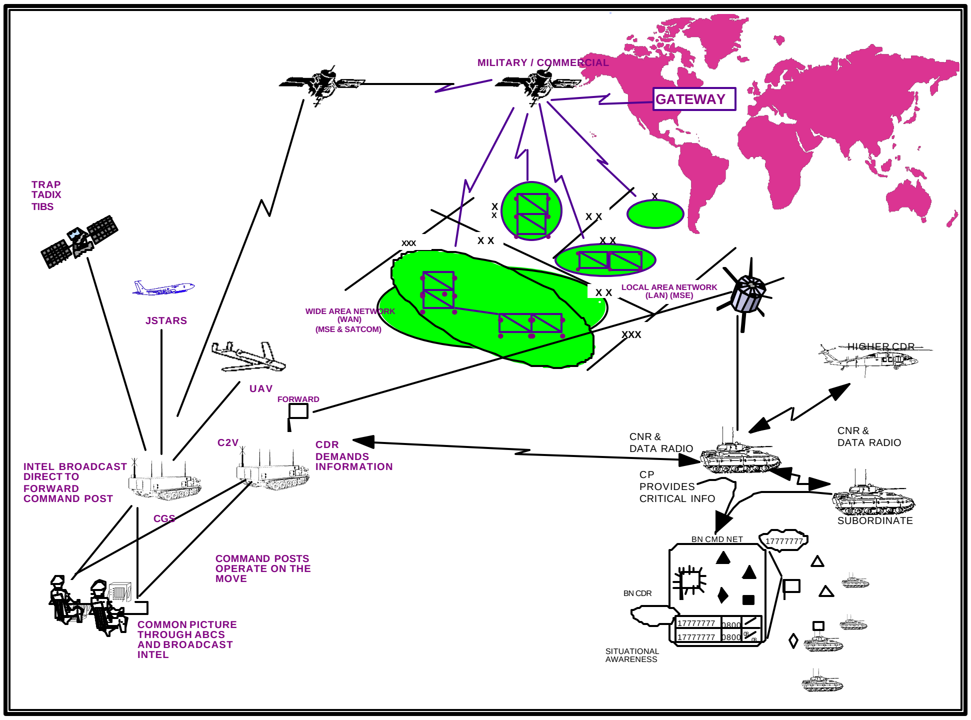


Figure 2.2-1. Integrated Architecture

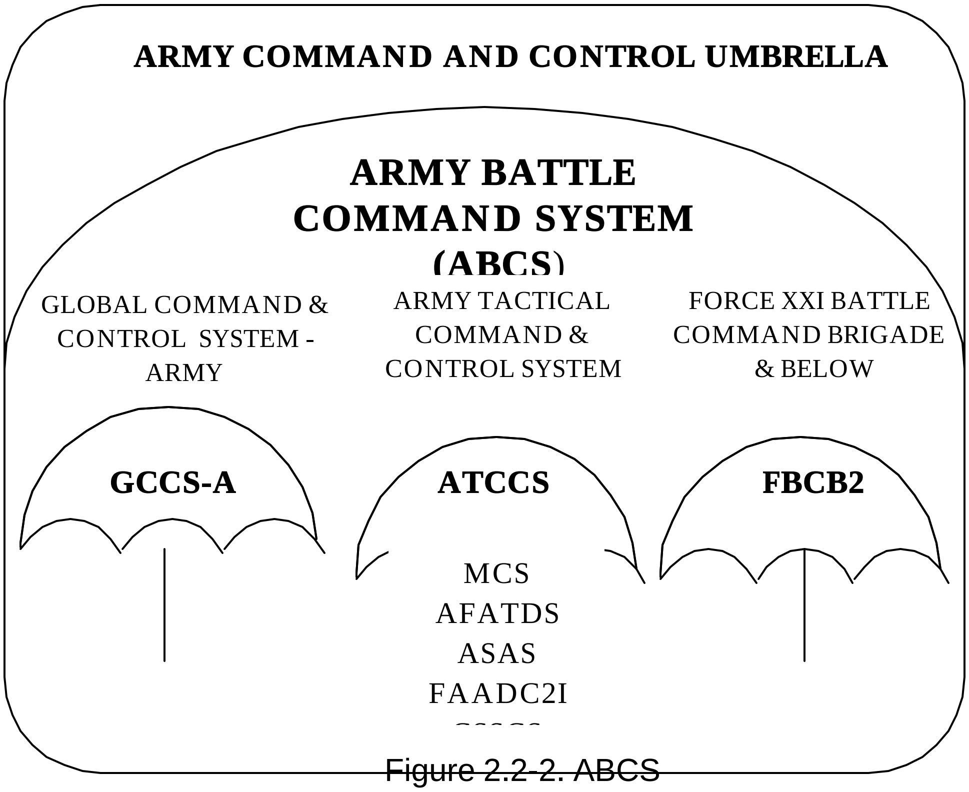


Figure 2.2-2. ABCS

2.3 EVOLUTIONARY MODERNIZATION. C4 modernization efforts will support the Army's Transformation Campaign Plan in support of the evolving Brigade Combat Team

(BCT) and, eventually, Future Combat Systems (FCS) by exploiting leap-ahead information transport, processing, and security technologies designed to provide commanders with overwhelming decision cycle superiority. Initially, gateways will be required to bridge the information flow among existing stovepipe systems. The essential elements that ensure C4 dominance are global, theater, and tactical area transport systems; tactical internet and battle command mobile platforms; and seamless, secure, adaptable information architectures.

The strategy seeks to address critical warfighter requirements common to any future operation. These requirements include the following:

- C2 on the Move: The dynamics of future operations will require continuous mission analysis and potential changes to plans. As a result, battle commanders require reliable C2 capabilities in garrison locations and during the deployment phase while enroute to the theater of operation. They also require the ability to exercise C2 from anywhere within the battlespace.

- Mobile and Flexible Command Posts (CPs): The ability to rapidly manuever a CP to keep pace with operations is essential. Satellite, wireless local area networks (LANs) and personal communications systems (PCSs) will enhance CP mobility.

- Situational Awareness: The force must have accurate, real-time knowledge of friendly, enemy, and noncombatant activities and locations.

- Reliable, Robust, and Survivable Communications Supporting Force Projection Operations: Seamless connectivity from sustaining base to the foxhole is the rule for future signal support to warfighting forces. The objective is to replace multiple, non-interoperable, stovepipe communications systems existing today. Users must have the ability to "unplug" from the network in the sustaining base and "plug-in" wherever they deploy.

Individual components of the Army's C4 Modernization Strategy are discussed in detail in Section 5.

2.4 PLANNED EVOLUTION OF CAPABILITIES. Access to and exploitation of timely information is a key element of the United States' future warfighting and crisis management capabilities, as well as its national competitiveness. The projected force-level multiplier advantage of information technology stands far above that of all other technical areas. Such capability greatly enhances the autonomy and survivability of individual units and quickly provides an advantage in any conflict, supporting early, decisive victory with minimal cost in assets and human life. Modernizing the Army to a technology-age force that is prepared to fight and win the information war encompasses many interrelated technologies and specialties with emphasis in two major areas: decisionmaking and seamless communications. The Army's technology objectives for C4 in "Decisionmaking" and "Seamless Communications" are presented in Tables 2.4-1 and 2.4-2, respectively.

Table 2.4-1. Technology Objectives for C4 – Decision Making

Technology Subarea	Near Term FY01-02	Mid Term FY03-08	Far Term FY09-16
Decision Making	- Terrain, environmental and event detection decision support software	- Automated maintenance of consistent, timely tactical picture in distributed C3	- Robust cooperation - Software agents dynamically support collaborative planning

Technology Subarea	Near Term FY01-02	Mid Term FY03-08	Far Term FY09-16
	- Automated flight plan guidance algorithms - Embedded software tools to enable real time collaborative planning in a three dimensional (3-D) virtual environment - Integrated and automated POS/NAV systems	systems - Automated situation awareness - Demonstrate joint distributed collaborative planning & assessment tools with 3-D visualization - Automated cooperative interaction between three to four systems - Robust precision POS/NAV	and execution - Dynamic immersive rehearsal planning and execution environment - Autonomous navigation in well-characterized terrain - Adaptive tactical navigation

Table 2.4-2. Technology Objectives for C4 – Seamless Communications

Technology Subarea	Near Term FY01-02	Mid Term FY03-08	Far Term FY09-16
Seamless Communications—Mobile Networking	- End-to-end quality of service - Develop/demonstrate new phased array for wideband on-the-move (OTM) operations - Demonstrate network self-organizing % routing protocols - Develop new airborne relay communications payload	- Fully networked, self-organizing OTM wireless for 15-20 nodes - 9.6 kbps MILSTAR, 5 Mbps wideband - Bandwidth management - Adaptive network protocols for mobility - Short-range wireless - Medium-range wireless - Demonstrate media access control layer protocol - Develop microcomponents & common architecture for microsensor processing -First-generation self-healing	- Fully networked, self-organizing, self-healing OTM wireless for hundreds of nodes - 9.6 kbps MILSTAR, 5-Mbps wideband - Bandwidth management - Adaptive network protocols for mobility - 3-D communications architecture - Significant use of commercial satellites - Spectrum agility - Autonomous network planning

Technology Subarea	Near Term FY01-02	Mid Term FY03-08	Far Term FY09-16
Seamless Communications—Unattended Sensor Networking	- Fast acquisition <50 ms - LPD/AJ - Large breadboard - Low-energy routing - Self-forming adaptive 10-node network - Integrated Meanderline antenna	- Uses <120,000 mWh over 40 days - Interradio range 200 m - Radio to gateway 3 km - Limited adaptive networking - Security architecture with medium LPI/LPD/AJ 20-dB processing gain - Radio size <6 cubic inches; 45 cubic inches with batteries - Monolithic antenna	- Provides FCS with remote access, reconfigure sensors, retrieve & transmit sensor data while OTM - Sensor-specific communications protocols, dynamic data routing algorithms, networking architecture, miniaturized RF components & antennas, power-efficient components, OTM dispersal, & sensor architecture configured for survivability - Demonstrate networked sensors & evaluate protocols - Uses <80,000 mWh over 60 days - Interradio range 400 m - Radio to gateway 10 km - Robust, self-forming, adaptive, 80-node network, scalable to 400 nodes with simulation - Seamless security, adaptable LPI/LPD/AJ
Seamless Communications—Information Assurance	- Access control - Intrusion detection & response - Security management - M&S - Attack/red team - Test event—Electronic Proving Ground, Ft. Huachuca, AZ	- Protected network 80% of the time - ABCS/WIN protect - Network access control—prevent malicious activity targets at computing & networking resources - Intrusion detection and response - Security management framework - Internet attack simulation - Security integration across tactical & sustaining base	- Protected network 80% of the time - Autonomous trusted agents - COA analysis - End-to-end encryption - Multilevel security - Self-detection of external attack - Auto vulnerability assessment - Security integration across tactical & sustaining base
Seamless Communications—Antennas	- JTRS at the halt multiband/OTM multiband -SHF OTM position tracker—achieved - EHF OTM position tracker—begin development - JTRS OTM antenna—four approaches, prototyped to be tested - Band-switch antenna—begin development - Low-cost phased array—validate multilayered PWB & surface-mount production techniques - Body-borne antenna—successful proof of concept	- Increase message-completion rate by 20% - EHF SATCOM for communications between FCS and EHF satellite - Ferroelectric/Ka-band PAAs - OTM multiband antennas - Altitude and heading reference system - Reconfigurable OTM band switched - Body-borne - First-generation vehicle conformal antennas	- Increase message-completion rate by 20% - Ferroelectric/Ka-band PAAs - VHF/UHF omnidirectional body-born, low profile, & conformal - Reconfigurable OTM band switched - Smart antennas - Micro antennas
Seamless Communications—Secure Personal	Adaptable communications; functional breadboard evaluation in operational	-Provides FCS dismounted soldier with secure multiband personal	-Provides FCS dismounted soldier with secure multiband personal

Technology Subarea	Near Term FY01-02	Mid Term FY03-08	Far Term FY09-16
Communication	environment to support network speed of service & message completion rate requirements under dynamic mobility & hostile electronic warfare conditions for dismounted infantry	communications with or without infrastructure -Brassborad universal headset -Wideband RF tunable front ends, reduced electronic signature, improved network availibility, INFOSEC module, multipath protection	communications, achieving low size, low weight, low power, & affordability -Production-ready universal headset -Low-power RF electronics; highly integrated, system-on-a-chip modem processing; improved, interference-resistant, softwear-programmable waveforms

NOTE: All acronyms in the table are defined in the List of Acronyms and Abbreviations.

3. THREAT SUMMARY

3.0 OVERVIEW. The threat can reduce the ability of C4 systems to perform mission-related functions by inflicting damage, forcing undesirable maneuvers, degrading system effectiveness, or affecting the quality of the transmitted data. A wide variety of weapons, mechanisms, and tactics may be employed by the enemy to threaten the survivability/reliability of C4 systems in and out of theater. Threats to U.S. Army C4 systems range from destruction by firepower from conventional and unconventional weapons to being rendered ineffective through electronic attack (EA). In addition, computer-based systems are subject to CNA that can result in unauthorized access to the network. These attacks can have a tremendous impact on the network (e.g., disruption by viruses and manipulation of the databases). The C4 systems can be detected by enemy ground combat forces; intelligence, surveillance, and reconnaissance (ISR) assets; electronic warfare (EW) assets, and through CNAs. Table 3.0-1 lists the primary threats to C4 systems survivability, along with the operational/physical effects on personnel and equipment.

Table 3.0-1 Primary Threats to C4 Systems

THREAT	OPERATIONAL	PHYSICAL	PERSONNEL	EQUIPMENT
Physical Attack Direct/Indirect Fire/ Missiles/ Aircraft/ Directed Energy	Loss of communications / loss of area communications connectivity	Destruction of personnel and equipment	Blind, wound, kill, force into cover/ movement	Communications equipment, nodes, computers, sensors
Offensive IO CNA/Unauthorized access EW Jamming Intercepting Spoofing Information Manipulation/ Destruction	Deny transmission of C2I and logistics information Enable enemy knowledge of plans and intent Allows enemy to disrupt/confuse execution Manipulate databases, corrupt databases, compromise data and information, deny, corrupt or lose service and effect confidence in data reliability	N/A	N/A	Communications equipment, networks, routers, and computers
Nuclear	Deny areas of operation; force movement, decon, personnel into protective equipment	Radiation, blast and electromagnetic pulse (EMP), loss of personnel and equipment	Sicken/wound, kill, force into protective equipment/ movement	Communications equipment, computers, and sensors
Biological	Force movement, evacuation of sick, deny use of equipment	Reduced effectiveness, loss of personnel, contamination	Sicken, kill, force use of protective equipment/ movement	Communications equipment, computers, and sensors
Chemical	Deny use of equipment and areas of operation, force movement, decon procedures, use of protective equipment	Incapacitating or lethal effects, contamination	Incapacitating or lethal to unprotected personnel, force use of protective gear	Communications equipment, computers, and sensors
Enemy ISR	Reduce freedom of communications systems operation (time and frequencies of radiation); force camouflage/concealment, sound/light discipline, IR suppression, frequent tactical moves	N/A	N/A	Communications systems, power sources, and CPs

3.1 THREAT TYPES. In general, threats can be grouped into non-terminal and terminal. Non-terminal threats do not routinely possess a capability to destroy systems (although, some non-terminal threats such as laser trackers can degrade/disrupt equipment or render a person blind; or viruses that destroy data within a system) but are used by enemy forces to support terminal threat elements. These non-terminal threats normally affect detection and early warning, target identification/tracking, electronic protect measures, fire or weapon control, and C2 systems. They can be land-, sea-, or air-based and are an integral part of the enemy's offensive and defensive forces. Their purpose is to supply position, speed, and heading information to the terminal threat units and affect U.S. forces' ability to effectively react to a threat's course of action. Terminal threats may be delivered from a wide variety of platforms including main battle tanks, infantry fighting vehicles, artillery, multiple-rocket launchers, ballistic missiles, cruise missiles, infantry, close air support (CAS), attack aircraft (rotary or fixed wing), directed energy devices, and computers. CNA are unique because they can be classified as both terminal and non-terminal threats. For example, unauthorized access into a network can result in the corruption/destruction of databases through the use of malicious viruses sent through the network. The unauthorized access may not result in the destruction of the C4 system hardware but could destroy the system's capability to function.

3.2 DETECTION AVOIDANCE THREATS.

3.2.1 **Intelligence, Surveillance, and Reconnaissance (ISR) Threat.** ISR is a process the enemy can be expected to carry out on a continuous basis, using every means at his disposal to detect, locate, and identify U.S. systems for attack, disruption/suppression, or avoidance. In this effort, the enemy will employ a variety of ISR techniques, devices, and platforms oriented toward exploiting the signatures of individual C4 systems. ISR devices and techniques will include passive and active surveillance means, as well as human intelligence gathering. They may be employed on ground-based, airborne, or space-based platforms.

3.2.2 **EW.** The mission of EW is to deny the enemy unrestricted use of the EM spectrum while permitting unrestricted friendly use of the same. The three categories of EW are illustrated and defined in Figure 3.2-1. They are electronic attack (EA), electronic warfare support (ES), and electronic protection (EP). EW is an integrated program of countermeasures. It is more than the sum of the individual categories. Elements of reconnaissance, firepower, communications, signal intelligence, jamming, direction finding, and deception can be used by an enemy to attack priority networks, nodes, and links to nullify, limit, or delay our use of C4 systems while protecting their own operational capability. Ground-based, airborne, and terrestrial-based platforms can provide an enemy the ability to intercept, locate, and jam tactical communications systems from the high frequency (HF) to super high frequency (SHF) portions of the frequency spectrum. The EW threat will continue to grow as C4 technologies are employed.

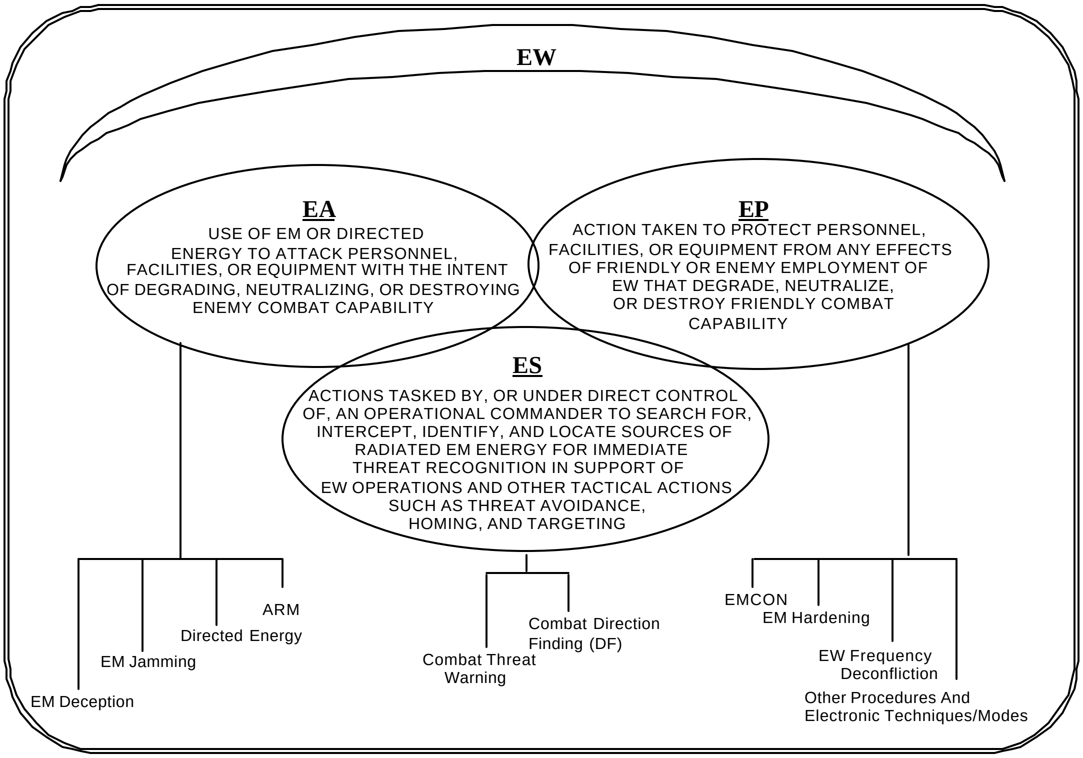

EW
EA
USE OF EM OR DIRECTED ENERGY TO ATTACK PERSONNEL, FACILITIES, OR EQUIPMENT WITH THE INTENT OF DEGRADING, NEUTRALIZING, OR DESTROYING ENEMY COMBAT CAPABILITY
EP
ACTION TAKEN TO PROTECT PERSONNEL, FACILITIES, OR EQUIPMENT FROM ANY EFFECTS OF FRIENDLY OR ENEMY EMPLOYMENT OF EW THAT DEGRADE, NEUTRALIZE, OR DESTROY FRIENDLY COMBAT CAPABILITY
ES
ACTIONS TASKED BY, OR UNDER DIRECT CONTROL OF, AN OPERATIONAL COMMANDER TO SEARCH FOR, INTERCEPT, IDENTIFY, AND LOCATE SOURCES OF RADIATED EM ENERGY FOR IMMEDIATE THREAT RECOGNITION IN SUPPORT OF EW OPERATIONS AND OTHER TACTICAL ACTIONS SUCH AS THREAT AVOIDANCE, HOMING, AND TARGETING
ARM
Directed Energy
EM Jamming
EM Deception
Combat Direction Finding (DF)
Combat Threat Warning
EMCON
EM Hardening
EW Frequency Deconfliction
Other Procedures And Electronic Techniques/Modes

Figure 3.2-1. Categories of Electronic Warfare

3.2.3 **IO Threat.** IO integrates all aspects of information to support and enhance elements of combat power, with the goal of dominating the battlespace at the right time, in the right place, and with the right weapons or resources. IO can be defined as continuous military operations within the military information environment (MIE) that enable, enhance, and protect the friendly force's ability to collect, process, and act on information to achieve an advantage across the full range of military operations. IO includes interacting with the global information environment (GIE) and exploiting or denying an adversary's information and decision capabilities. IO is conducted across the full range of military operations, from operations in garrison, through deployment, to combat operations, and continuing through redeployment upon mission completion. The threats to the information infrastructure are genuine, worldwide in origin, technically multifaceted, and growing. They come from individuals and groups motivated by military, political, social, cultural, ethnic, religious, or personal/industrial gain. The globalization of networked communications creates vulnerabilities due to increased access to information infrastructure from many points around the world. Threats against computers, computer systems, and networks vary by the level of hostility, technical capabilities, and motivation. Offensive IO is defined as actions taken to achieve information superiority by affecting adversary information, information-based processes, information systems, and computer-based networks while defending one's own information, information-based processes, information systems and computer-based networks. As it relates to C4 systems, the offensive IO threat focuses on intercepting, exploiting, corrupting, and/or destroying systems or data (in existing databases or being exchanged between databases). Adversaries have several options to influence or attack opposing C4 systems. This can either be accomplished through physical destruction or CNAs. CNAs can also be designed with a delayed effect, such as corrupting a database or controlling a program, as well as immediate actions to degrade or physically destroy. Examples include the following:

- unauthorized access to classified or sensitive military information,
- insertion of malicious software to cause a computer to operate in a manner other than that intended by its users (this category includes computer viruses, logic bombs, and programs designed to bypass protective programs),
- corruption of data through use of malicious software or alteration of data,
- sowing of disinformation,
- lengthening of the Army's command decision cycle,
- misdirection of U.S. forces, weapons, or sensors,
- delay or prevention of the development or deployment of Army information systems, and
- withholding of battlefield or other situational information.

3.3 HIT, PENETRATE, AND KILL AVOIDANCE THREATS.

3.3.1 **Direct/Indirect Fire Threat.** The direct/indirect-fire threat includes all ground-based or air-delivered weapons that might be employed against C4 systems, such as artillery, rockets, tank cannon, small arms, explosives, and directed energy weapons (DEWs). The employment of special operations forces (SOF) is also included because of the tremendous damage they can inflict on a deployed C4 system.

3.3.1.1 Overall Attack. C4 systems will come under attack by all types of direct and indirect fires as they move to support the maneuver force engaged with the enemy. The increased emphasis on disrupting information systems that support C2 makes C4 systems high-priority targets that will be engaged when detected. Direct hits by large- caliber weapons, such as tanks, rockets, and cannon artillery, will result in destruction of all but the hardest targets. Submunitions, such as improved conventional munitions (ICMs) and dual-purpose improved conventional munitions (DPICMs), provide artillery systems with the ability to saturate the target area with bomblets designed to be lethal against ground vehicles and personnel. At the other end of the spectrum are the “smart” munitions delivered by various means. These include terminal homing and sensor-fused munitions that rely on multiple sensors to select a suitable target, arm themselves, engage, and damage or destroy the target. Fragmentation from indirect fires is one of the greatest threats to C4 systems' soft-skinned vehicles and the dismounted soldiers supporting them. Small arms, machine guns, and medium-caliber weapons, such as those mounted on armored vehicles, also pose a threat to C4 systems and crews that are not provided armor protection.

3.3.1.2 Rear Attack. In rear areas, the most significant threat is attack on fixed CPs and communications nodes by enemy SOF or indigenous terrorists. The isolation of most C4 systems and the limited size of the crew increase the vulnerability and possibility of attack. The key characteristics of SOF/terrorists are that they can covertly engage C4 systems throughout the battlespace. Employing “hit and run” tactics, they are very difficult to counter and defeat. They will be keyed to the presence of C4 systems via visual identification of antennas, acoustic, and activity signatures.

3.3.2 **DEW Threat.** The three principal divisions of directed energy include lasers (low and high energy), high-power radio frequency (RF) directed energy weapons (DEWs), and particle beams (charged and neutral). Whereas conventional weapons rely upon a projectile, DEWs utilize subatomic or electromagnetic (EM) particles impacting on the target at or near the speed of light. These weapons produce casualties and disrupt or damage equipment by focusing energy on the target. Using passive aiming systems, DEWs strike with no signature and require no computation of lead. Although DEWs have not been a factor in previous conflicts, they have the potential to pose a serious threat in the future. The likeliest battlefield employment of DEWs is the use of lasers and microwaves as anti-sensor weapons to disrupt or damage visible, infrared (IR), and microwave sensors.

3.3.3 **Antiradiation Missile (ARM) Threat.** C4 systems that employ active emitters are susceptible to detection by enemy ISR means and to attack by ARM. The modern ARM is capable of being launched at long distances and homing on a RF emitter with great accuracy. The ARM threat to forward area, corps, and theater C4 systems, which depend upon active radio emitters to exchange information and direct action, must be countered if the systems are to survive and accomplish their mission. Because of the sophisticated target discrimination measures employed by modern ARMs, countermeasures rely on solutions that are difficult to implement, offer a solution for only part of the threat, or are counter-productive to the mission. Current passive countermeasures are insufficient to counter the rapidly advancing ARM threat. Sophisticated decoys capable of drawing off ARMs are costly and of unproven effectiveness.

3.3.4 **Cruise Missile (CM) Threat**. The effectiveness of U.S. CM in Desert Storm did not go unnoticed by potential adversaries. U.S. forces deployed in future conflicts to almost any area of the world are likely to face a significant threat in the form of extremely lethal weapons carried by highly accurate, long-range CMs. CMs have generally not been targeted at tactical units, but technology advances and cost reductions could change that in the future.

3.3.5 **Tactical Ballistic Missile (TBM) Threat.** Currently, there are at least 25 countries with a TBM capability. The numerous advantages of TBMs favor their use and proliferation as an affordable alternative to more expensive weapons systems. A serious potential problem is posed if the current threat TBM technology, which has poor accuracy, is combined with modern Global Positioning System (GPS) technology to provide credible targeting accuracy. This deadly combination could give rise to a long-range strike capability that even poorer nations could obtain, develop, and afford. TBMs can carry weapons of mass destruction that have the potential of holding the U.S. at political as well as military risk. These weapons are generally not targeted at tactical units but rather focus on disrupting lines of communication and logistics or achieving strategic objectives. Nonetheless, TBMs are potential delivery means for payloads (e.g., DPICM-type bomblets or nuclear, biological, and chemical [NBC] payloads), which can threaten C4 systems, whether deliberately or inadvertently targeted.

3.3.6 **Chemical and Biological (CB) Threat.** More than 25 countries are currently known or suspected to possess chemical weapons capabilities. Additionally, a number of other nations are suspected of possessing biological warfare agents. CB weapons affect personnel almost exclusively, although the presence of these agents on equipment may deny its use for mission performance. Chemical agents may cause corrosion of equipment surfaces, seals, and filters, as may the means used to decontaminate the equipment after a chemical attack. Such corrosion may have a highly damaging, although possibly delayed, effect on electronics, optics, and computers.

3.3.7 **Nuclear Threat.** The probability of exposure to nuclear attack is less than that of exposure to a chemical attack because nuclear weapons' ownership is restricted to a much smaller group of nations. However, there has been a concerted effort on the part of several countries to develop this capability. These countries are known to possess TBMs capable of delivering nuclear as well as CB warheads to targets at long ranges. Although they will likely never achieve a nuclear arsenal in the numbers or sophistication of the major powers, these nations might be more willing to employ nuclear weapons. Given C4 systems' permeation of the battlespace, they must be protected against the effects of nuclear attack in order to survive and accomplish their mission. Nuclear weapons may destroy or neutralize the effectiveness of equipment and personnel through a variety of initial and residual effects, as illustrated in Figure 3.3-1.

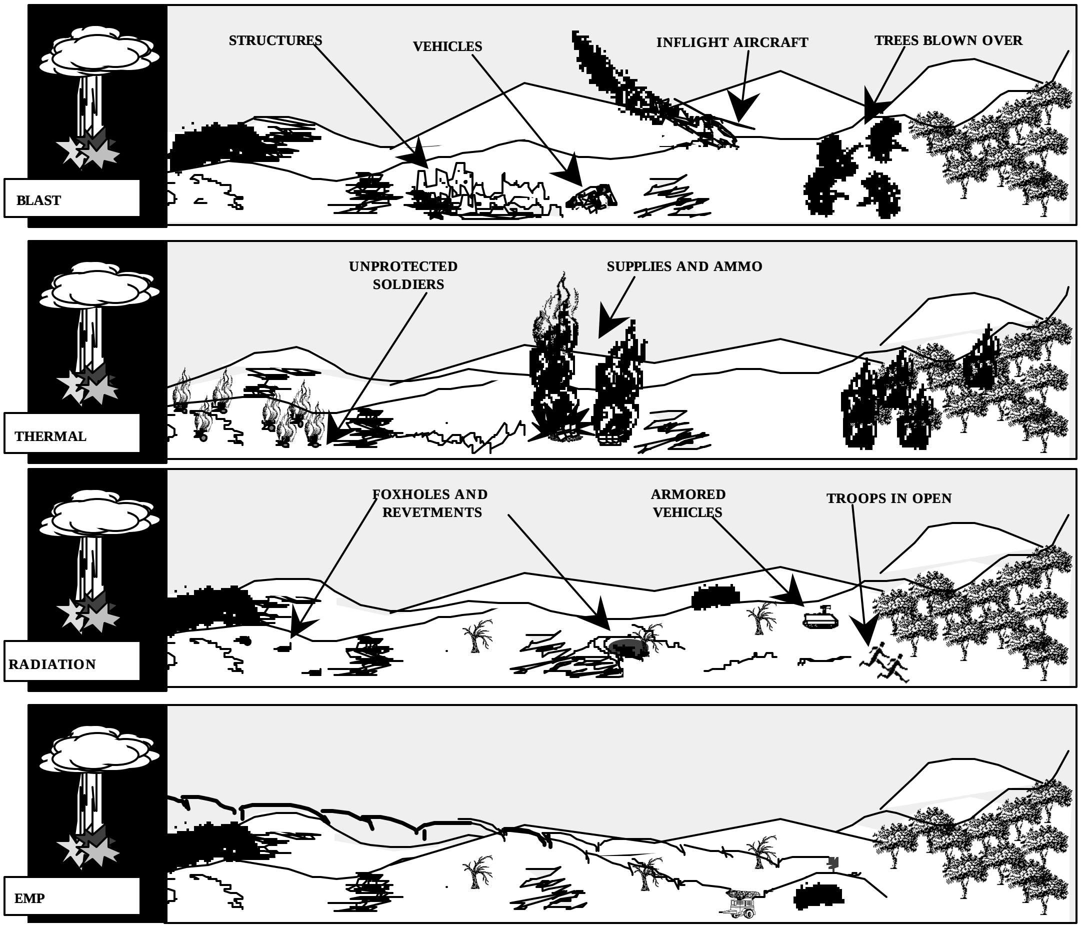


Figure 3.3-1. Nuclear Weapons Effects

4. SURVIVABILITY ANALYSIS OF C4 SYSTEMS

4.0 GENERAL. As noted in section 1, survivability is defined as "the capability of a system and crew to avoid or withstand a manmade hostile environment without suffering an abortive impairment of its ability to accomplish its designated mission." The key words in this definition are "avoid and withstand." These terms are measures of a system's susceptibility and vulnerability to the hostile environment. Susceptibility can be divided into three general categories of threat activity: (1) detection, identification, and tracking; (2) engagement; and (3) effect(s). Susceptibility of a C4 system is influenced by such factors as the system's design (e.g., signature and maneuverability), tactics used (e.g., terrain masking to avoid detection), and survivability equipment (e.g., firewalls). Vulnerability is determined by the enemy's knowledge of potential platform susceptibilities and his capability in recognizing and attacking a system with these susceptibilities.

4.1 SUSCEPTIBILITY SUMMARY.

4.1.1 **<u>Detection Susceptibility</u>.** The susceptibility of C4 systems to enemy ISR is a major survivability consideration. IR, acoustic, RF, and visual sensing technologies are mature and widespread. C4 systems throughout a theater will be subject to enemy efforts to locate and identify them for intelligence gathering, disruption, or destruction.

4.1.1.1 IR Signature. C4 systems' internal temperature variations form visible patterns that provide significant IR imaging. The thermal signatures of C4 systems consist mainly of solar heating, engine and generator operations, and friction. Solar heating affects the surfaces of the vehicle and highlights the target's overall shape. These shape cues are recognizable out to medium and long ranges, depending on the sensor's resolution. In addition, personnel heaters either create heat or trap engine heat. The engine, generator, heated compartments, and exhaust outlets are comparatively hot and typically easily detected at longer range. Frictional heat is produced by the moving parts of vehicles. Thermal signatures are highly variable due to solar heating, engine operation, frictional heating, and atmospheric conditions (e.g., falling precipitation or fog). Furthermore, when dismounted, the soldier becomes susceptible to the adversary's ISR techniques. Therefore, it is important for both materiel and soldier survivability to consider the situations arising from soldier and equipment interaction. For example, the overall signature of a vehicle may change with the presence of nearby infantry or exposure of a human head.

4.1.1.2 Acoustic Signature. C4 systems present a wide variety of noise sources detectable on a modern battlefield—engine and generator noises, vehicle mechanical systems, tracks or tires, and vibrating structural components. The acoustic signature of a tactical vehicle or generator can propagate through the air over considerable distances. This propagation is not line-of-site (LOS) dependent, may work better at night, and can use human hearing as the detection system. Mechanical and electronic systems may be more sensitive and can be used to extract additional information. Under ideal circumstances and with proper equipment, acoustic signatures provide sufficient information for not only detection and identification, but also targeting of the sound source. On the battlefield, the maximum detection distance is subject to considerable variation as a result of atmospheric and terrain conditions between the sound source and the detector and between the background noise levels and the detector's performance characteristics. Major sound attenuators are geometric spreading, atmospheric absorption, the reflection plane, refraction due to temperature and wind gradients, shielding by barriers, and foliage attenuation.

4.1.1.3 Transmission/RF Signature. C4 systems have unique transmission/RF signatures as they use the EM spectrum to support C4 requirements. Further, the expanded use of the EM spectrum increases the susceptibility to detection and interception by enemy collection systems. The evolving reliance on automated information processing techniques is all but essential for the Army's modern C4 systems. However, this reliance on automated systems also incurs a penalty as enemy forces can be expected to employ all means to intercept and exploit C4 traffic. Specifically, the force's information systems and communications are susceptible to interception, jamming, CNAs, unauthorized access (intrusion), disruption, and spoofing.

4.1.1.4 Visual Signature. C4 systems will continue to rely on cover, concealment, camouflage, and light discipline to avoid detection and acquisition. However, the use of counter-ISR places an additional burden on the individual soldier and may reduce his/her operational effectiveness.

4.2 SURVIVABILITY—DECISIONMAKING. C2 is extremely susceptible to detection and vulnerable to disruption. CPs are cumbersome and easily detectable by their visual, electronic, and IR footprints. With limited means to disseminate information throughout the CP, dispersion to reduce this signature is difficult. Current CPs must often use wire strung between elements of the CP or large, highly visible antennas. The wire networks are resource and manpower intensive, provide limited capacities, and are time consuming to install and recover. Radio systems for internal CP communications produce a large, easily detectable signature. A large CP will have numerous antennas erected, making visual detection a probability. Most antennas are omnidirectional and easily detected by enemy EW assets. Power sources that supply CPs emit a significant IR signature. Additionally, CPs at division and higher have an extensive physical footprint and require long setup/teardown times. C2 elements at brigade and below face these as well as other problems. Currently, automated systems to assist commanders at this level are limited. Information is still passed mostly by voice, through face-to-face exchanges of information, or by maps and map overlays. Only limited capability to obtain or process digital information such as friendly and enemy locations is available. While the GPS provides units with more accurate and timely friendly and threat positions, units still rely on accurate estimates and voice transmittal. Both actions are time consuming and subject to degradation during intense combat situations. Additionally, during movement, CPs are generally limited to manual tracking of unit movements and voice communications. These limitations hamper the commander's ability to operate in a timely manner. Although these shortcomings do not lead to a specific susceptibility or vulnerability issue, they do make the lower echelon C4 system more susceptible to overall threat EW/countermeasures. As the digitization effort is integrated into a lower echelon C4 system, offensive IO will become a more critical consideration. Lower echelons may have less capability to detect offensive IO incursions and become more susceptible and vulnerable to offensive IO effects. One concern that effects survivability at every level relates to cosite interference. As the digitization effort is expanded, there is a corresponding increase in the utilization of the EM spectrum. The resulting friendly interference may be as debilitating as any threat offensive IO actions if the United States does not take steps to maximize effective use of the EM spectrum.

4.3 SURVIVABILITY: SEAMLESS COMMUNICATIONS. The fielding of mobile subscriber equipment (MSE) has done much to improve the survivability of the area communications network in the corps area. The replacement of single threaded communications links with a robust grid network was a giant step forward in survivability. However, many survivability issues remain. The MSE architecture was based on a network of relatively evenly spaced communications nodes. In theory, the survivability of the network increases as the number of nodes increases. In the fully deployed European scenario, a very robust, survivable network could be envisioned. The network that resulted during the Iraq War covered such an extended area, with relatively few nodes, that the network's survivability was often in jeopardy. Future operations, particularly in support of FCS, will require transmission of large amounts of data. Limited means of data transmission currently exist. MSE is now being upgraded with a packet switch network overlay that will provide improved capacity for data flow; its capacity, however, will not meet the full requirement and will not reach the lower echelons where data will be needed. The capability to exchange data across all battlefield functional areas (BFAs) and echelons is key to enhanced situational awareness, and, thus, survivability of the force. The Single-Channel Ground and Airborne Radio System (SINCGARS) has limited data capability; however, but this capability is being improved through ongoing enhancements to the radio and fielding of improved data-transfer modems. Despite these improvements, there will be a serious shortfall in data-transfer capacity to support digitization goals. As the Wide-Area Network (WAN) is improved and expanded, it becomes more susceptible and vulnerable to threat offensive IO. Expanding the number of paths and nodes provides more entry points for the threat to initiate CNAs against the overall network and provides the threat with more opportunities to gain information.

4.3.1 **Survivability: Seamless Communications—Mobile Networking.** Modern combat operations demand movement. Forces on the move, particularly those engaged in maneuver, require access to real-time information just as much or more than when they are stationary. In order to maintain situational awareness and survive on the fast-paced battlefield, warfighters must have survivable communications that have the capability and capacity to keep them connected to the information sources and processing power that they have in their fixed CPs. Current mobile communications do not meet the transmission capacity requirements envisioned for future automated systems. New systems approaching this capability will, however, become beacons for threat offensive IO. While this area is no more susceptible or vulnerable to offensive IO than the other C4 functional areas, the effects of an offensive IO attack in a mobile situation can be more devastating because of the impact on the moving element. An attack on a fixed location that migrates through the network to the mobile sites could cause particularly great confusion.

4.3.2 **Survivability: Seamless Communications—Unattended Sensor Networking.** The success of the FCS concept is heavily dependent upon the ability to provide an assured networked communications grid. This grid will provide FCS with remote access to its organic sensor systems, the ability to reconfigure those sensors remotely, a self-healing capability in the event of network or sensor damage or destruction, and the ability to provide wireless connectivity for hundreds of nodes while on-the-move (OTM). This developing network will require very stringent safeguards to ensure FCS cannot be rendered ineffective by depriving the system of its "eyes" through offensive IO that destroy or disrupt the sensor network.

4.3.3 **Survivability: Seamless Communications—Information Assurance.** Due to the present and ever-increasing dependence upon automated information systems, IA has become critical. In both war and peace, computer systems and networks on which units rely are vulnerable to attack. On the battlefield, reliance on an extensive and potentially fragile communications infrastructure presents a vulnerability that entices exploitation. CNAs resulting in unauthorized access to C4 systems provide an adversary with the opportunity to not only disrupt, manipulate, or destroy databases, but also to know everything known to the friendly commander. CNAs can destroy situational awareness (SA), a cornerstone of successful operations. The key is to prevent the threat from accessing the network routers and system hosts. There is a wide range of methods and techniques for gaining access to network routers and system hosts. Network attacks may attempt to exploit the following:

- Default Services: Router services enabled by default may be exploited.
- Address Resolution Protocol: A router may be deceived as to the actual addresses of local hosts or other routers, with the result that the system may send messages to unauthorized hosts.
- Trivial File Transfer Protocol (TFTP): Router configuration may be modified to send system files to an unauthorized destination.
- TELNET Service: The password of the router manager may be stolen by remote login.
- Internet Protocol (IP): The originator of an illegal packet or session may misrepresent himself as a legitimate user (also known as “IP spoofing”).
- Access Control List: An improperly configured access control list may permit unauthorized traffic through the router.
- Established Keyword: This feature can be bypassed so that a client system is able to initiate an otherwise prohibited connection to the server.
- IP Fragmentation: IP fragments may be used to bypass the router’s filtering mechanism.
- IP Source Routing: Altering IP source routing may allow prohibited communications.
- Internet Control Message Protocol (ICMP): An illegal host purporting to be a router may be able to send an ICMP gateway redirect message to another router, allowing messages to be sent to the illegal host.
- Routing Information Protocol: A router may accept bogus routing information.
- Simple Network Management Protocol (SNMP): Information may be gathered about a router that allows an attacker to modify that router’s configuration.
- Terminal Access Controller Access Control System (TACACS): If TACACS is bypassed, an authorized user could gain access to the router.

- Open Shortest Path First (OSPF): A router may temporarily accept bogus routing instructions.

Host attacks may be launched against the following:

- The X-Windows System: Unauthorized users can covertly capture user keystrokes and the user's monitor display.

- The Network File System (NFS): Unauthorized users can use the commercial internet to export an NFS file system to their own machine.

- Secured Teletypewriter (TTY): This is a configuration attribute that may allow unknown users to log on to the target system with system-level ("root") access privileges.

- Null Shell Field: No default is specified in the login account allowing unauthorized users to easily login.

- World-Writable System Files: A configuration error that allows any user to modify sensitive system configuration files.

- Duplicate User Identifier (UID): An administrative error in which the same UID is assigned to two or more users. Any such user can then access the files of colleagues having the same UID.

- Changed Files: The modification by an attacker of system files that should remain static.

- Simple Mail Transfer Protocol (SMTP): A wide variety of vulnerabilities are known to exist in standard SMTP-based E-mail software utilities, such as UNIX Sendmail.

- User-to-User Decode (UUDECODE): Invoked via Sendmail, UUDECODE can be used to create arbitrary Superuser Identifications (SUIDs), allowing unauthorized persons to execute commands with "root" privilege.

- Trivial File Transfer Protocol (TFTP): Allows a user to retrieve any word readable file anonymously (i.e., without password authentication).

- Anonymous File Transfer Protocol (FTP): This configuration error permits anonymous users to retrieve or modify sensitive system files, such as the system's password file.

- Network Information System (NIS): Password files may be stolen and subjected to off-line cracking attempts.

These intrusions may be initiated during peacetime or at any point in an operation. Intrusions can be initiated from the top down or bottom up. In either case, the effect on a network can be devastating. It is even possible that a military system could come from the factory with an embedded logic bomb or virus; new commercial disks used by government agencies have been found to contain a virus upon delivery from the factory. While the use of Information Security Systems (ISSs) is becoming more prevalent, there is still a heavy reliance on administrative procedures. These procedures are difficult to implement and almost impossible to monitor on a chaotic battlefield. Some additional security improvements have been implemented and do provide security within a stove-piped system, but at the expense of reduced bandwidth, dedicated hardware and software, and a consistent inability to share data with other systems.

4.3.4 **Survivability: Seamless Communications—Antennas**. At present, both CPs and command vehicles will have numerous antennas erected, making visual detection a probability. An enemy can be expected to use any means available to destroy or disrupt an opponent's effective function of command. In battle, this may translate to engagement and destruction of identified CPs or command vehicles with direct or indirect fires as a hasty means of neutralization vice more time-consuming forms of attack (e.g., EA) or exploitation. The result of such destruction is usually long lasting; in addition to physical destruction, the loss of key personnel associated with command vehicles and CPs can be debilitating to a maneuvering unit. Most antennas currently in use are omnidirectional and easily detected by enemy EW assets. Particularly in cases where an enemy identifies a U.S. CP when not actively engaged, his most probable course will be to target the asset for later disruption or destruction, while seeking, via IO, to exploit the asset for as long as possible by gaining intelligence on friendly intentions or disposition.

4.3.5 **Survivability: Seamless Communications—Secure Personal Communications**. The dismounted soldier will require low-power, lightweight communications capability to ensure seamless connectivity with emerging military upper echelon communications systems and organic tactical sensors. Currently, the few personal communications systems available to Army forces employ the fixed cellular infrastructure requirements common to currently existing commercial cellular land networks. These networks are highly susceptible to detection, present security issues, and are subject to disruption not only by deliberate enemy action, but also by weather and atmospheric conditions. Future systems will require advances in multipath performance, as well as antijam/low probability-of-detection (LPD) protection. Safeguards must be built into the future networks to limit the effectiveness of threat offensive IO.

4.3.6 **Survivability: Seamless Communications—Reachback.** In order to ensure seamless communications from the Pentagon to the foxhole, the evolution of both theater and global broadcast systems which are secure, adaptable, and robust, as well as IO-resistant interfaces between tactical and global communications systems are an imperative. These systems must be operable over the entire combat and garrison continuum, providing multilevel, multimedia data and information connectivity throughout all phases of military operations.

4.4 C4 VULNERABILITY TO NBC. C4 is particularly vulnerable to the effects of NBC attacks. The lack of over-pressurized vehicles to support C4 systems, reliance on external power sources, and a lack of NBC protective covers severely limit operations in a contaminated environment. C4 systems, once contaminated, are very difficult to decontaminate. In many cases, the lack of an adequate means of decontamination prevents use of the C4 system for the duration of an operation. The necessity for soldiers to operate in NBC protective gear results in degradation in effectiveness and efficiency. Additionally, battlefield contaminates could affect C4 systems circuitry.

5. SURVIVABILITY ENHANCEMENTS

5.0 GENERAL. Survivability measures and procedures must both actively and passively preserve the confidentially, integrity and functionality of C4 systems. The evolution of battlefield C4 systems into the 21st century began with the current systems as a baseline. In order to preserve current investments, a step-by-step block improvement approach to modernizing legacy systems is being utilized. The combination of advanced technology/technology demonstrations (Figure 5.0-1), system upgrades, and the development of new technologies provide the flow of C4 modernization that contributes to survivability enhancements. By using a variety of new techniques and technologies, as well as introducing new applications of proven technologies, the survivability of information flow on the battlefield can be ensured, and the survivability and effectiveness of the force will be enhanced. This section focuses on enhancements that improve survivability of C4 systems. A point that must not be overlooked is that the survivability of C4 systems impacts the probability of other systems surviving because of the increased situational awareness capability that C4 systems provide.

Table 5.0-1. C4 Demonstration and System Summary

Advanced Technology Demonstration (ATD)	**Advanced Concept Technology Demonstration (ACTD)**
• Agile Commander • Multifunctional On-the-Move Secure, Adaptive, Integrated Communications • Tactical Command and Control Project	• Rapid Terrain Visualization • Theater Precision Strike Operations
Technology Demonstration (TD)	
• Battlespace Tactical Navigation • Collaboration Technology for the Warfighter • Command and Control for Joint Intelligence, Surveillance & Reconnaissance • Warrior/Platform Command & Control • Army Communications Integration & Cosite Mitigation • Network Management Assistant • Army.com • Smart Sensor Communications Networks • Tactical Information Assurance Technology • Antennas for Communications Across the Spectrum • Advanced Antennas • Dismounted Warrior Command, Control, Communications, Computers, & Intelligence C4I Technologies • Universal Handset • On-the-Move Tactical Satellite Communications • Next-Generation Satellite Communications	

5.1 TECHNOLOGY PROGRAMS LEADING TO ENHANCED SURVIVABILITY: COMMAND AND CONTROL.

5.1.1 **Agile Commander Advanced Technology Demonstration (ATD) (2000-2004).** The Agile Commander ATD demonstrates a dispersed, highly mobile command post that provides the commander with continuous, responsive, proactive, real-time battlespace management information during both stationary and mobile operations. By leveraging Defense Advanced Research Projects Agency (DARPA) initiatives (Command Post of the Future and Global Mobile [GloMo]) and ARL's work in advanced battlefield planning processing technology, the Agile Commander will provide a scalable and reconfigurable C41 multifunction operator environment with access to all command post information. This program will integrate the capabilities of the Multifunctional On-the-Move Secure, Adaptive, Integrated Communications (MOSAIC) ATD for mobile demonstration.

5.1.2 **Rapid Terrain Visualization (RTV) Advanced Concept Technology Demonstration (ACTD) (1997-2001).** The goal of this ACTD is to demonstrate capabilities to collect data and generate high-resolution digital terrain databases in support of crisis response and force projection operations within the joint force commander's timeline. The commander will be capable of integrating terrain databases with current operational information, producing the ability to manipulate and display these integrated databases in support of operational planning. The ACTD evaluates source data collection, digital terrain database generation and tailoring, dissemination, and applications software.

5.1.3 **Battlespace Tactical Navigation (BTN) Technology Demonstration (TD) (1999-2003).** Accurate position/location information is a key component of situational awareness. BTN will develop technology and integration concepts to improve navigation systems. Enhancements to the existing GPS include deployable pseudolites to enhance GPS survivability in a hostile electronic countermeasures (ECM) environment as well as the incorporation of antijam GPS technology. Redundant position/navigation capabilities will be provided via devices tailored to platform and mission. Improved algorithms will minimize initial database registration errors and enhance GPS dependability.

5.1.4 **Collaboration Technologies for the Warfighter TD (1999-2002).** The goal of the TD is to dramatically improve commanders' abilities to shorten decision cycles by compressing the observe—orient—decide—act loop. This TD is unique in combining leading-edge commercial-off-the-shelf (COTS) products with research products under development for the virtual environment and adapted to work with emerging battlefield visualization technologies. The technical concept is to push technology integration from insights gained in battlefield visualization, intelligence, low-bandwidth video teleconferencing, writing analysis, and icon recognition optical character reader (OCR) into a collaboration or decision-aid toolset.

5.1.5 **Command and Control for Joint Intelligence, Surveillance, and Reconnaissance (C2JISR) ACTD (2000-2003).** The goal is to develop a common C2 and intelligence object-oriented, distributed tactical database for the brigade to improve C2 battlefield visualization and course of action (COA) development and analysis. Intelligence agents will provide access to and correlation of battlefield information, thereby enhancing situational awareness and reducing information overload of workstation opperators.

5.1.6 **Warrior/Platform Command and Control TD (2005-2008).** This TD will develop and demonstrate enhancements of C2 tools available to the warfighter, emphasizing digital C2 products and tools that are useable across brigade and below platforms, including the dismounted warrior. Candidates for inclusion are as follows: low-power electronics architectures, hands-free human—computer interface, knowledge-based situational awareness, distributed collective battle planning, mission rehearsal and distance-based training, automated COA determination, and precision sensor tasking. The program will also develop capabilities for units to conduct instrumented tactical engagement simulations to support spiral development, training, operations rehearsal, and post-operation after action reporting.

5.1.7 **Theater Precision Strike Operations ACTD (2000-2001).** This program develops and demonstrates a significantly improved capability to synchronize, coordinate, deconflict, and employ the deep-strike assets of the Joint Land Force Component Commander (JFLCC) with joint and coalition assets between the forward line-of-own-troops (FLOT) and the forward boundary. A theater Enhanced Deep Operations Coordination Center (EDOCC) with enhanced C4 and strike-planning processes, to include Army Tactical Command and Control System (ATCCS) enhancements, GCCS-A integration, visualization tools, and connectivity with coalition forces, will be developed. Using the capabilities of the Deep Operations Coordination Center (DOCC), the JFLCC will be better able to employ current, as well as future systems, for effective precision deep strike operations.

5.2 TECHNOLOGY PROGRAMS LEADING TO ENHANCED SURVIVABILITY: COMMUNICATIONS—MOBILE NETWORKING.

5.2.1 **Multifunctional On-the-Move Secure Adaptive Integrated Communications (MOSAIC) ATD (2000-2004).** Army transformation to the Objective Force requires mobile forces and command and control capability while on the move. The goal of this program is to provide integrated, self-organized, OTM networked communications to support short-range <1 km), medium-range <10 km), and extended-range (>10 km) wireless elements capability. MOSAIC has three major areas of focus: (1) bandwidth management—scaled bandwidth request based on precedence, support of bandwidth reservation, proxies to drive bandwidth-aware applications, and the addressing of IP quality of service (QOS) over tactical wireless links; (2) adaptive network protocols to support infrastructure mobility—ad hoc network protocols to support self-initializing, self-healing, adaptive, mobile networks while addressing security; and (3) enhanced communications capability through the integration of commercial- and DoD-leveraged technologies—products from internal 6.2 efforts, DARPA products, and commercial products will be leveraged and integrated to demonstrate this mobile capability. Mobile protocols will be integrated into a prototype short-range wireless system followed by integration of mobile protocols into a prototype, medium-range wireless system and an airborne relay. An initial limited field demonstration will be performed, and a laboratory demonstration will be conducted of the integrated protocols, agents, and proxies that provide bandwidth management and support IP QOS and ad hoc networking. All this will culminate in an integrated demonstration with airborne relay, space-based assets, and terrestrial systems.

5.2.2 **Army Communications Integration and Cosite Mitigation (CICM) TD (1997-2001).** The CICM vision is to enable communication systems integration of the future Joint Tactical Radio System (JTRS) into Army tactical platforms through the application of JTRS ancillary communications products developed under the CICM and Antenna Communications Across the Spectrum (ACAS) Science and Technology Objective (STO).

The objectives of the CICM program are threefold. First, develop separate very high frequency (VHF) and ultrahigh frequency (UHF) multiplexer prototypes using advanced cosite mitigation technologies to reduce the cosite interference problems that occur when multiple radios are integrated within a mobile communications command post platform. Second, develop wideband power amplifiers that eliminate dissimilar legacy radio amplifiers and their logistics, training, and maintenance infrastructures. Lastly, the TD seeks to develop a Joint Tactical Radio System (JTRS) interface for the wideband power amplifiers and multiplexers to facilitate operation with the future JTRS radio. Field tests and the JTRS Integration and Cosite Laboratory will be used to evaluate CICM products using the multiband JTRS OTM antennas developed earlier under the ACAS STO.

5.2.3 **Network Management Assistant (E-Assistant) TD (2005-2007).** The goal of this effort is to provide a network-oriented, automated, self-healing, global network management capability that leverages the commercial base technology and dynamic readdressing and management and develops algorithms and rule sets to provide solutions optimized for tactical operations. E-Assistant will mature the next generation of tools and algorithms required to provide comprehensive network planning, centralized management, smart allocation of throughput (network telemetry), performance management, global interoperability, spectrum engineering and control, reconfiguration (to include adjustment, corrections, and reallocations), automated monitoring of tactical systems, detailed planning engineering capable of engineering 100% of global information systems, and high-level planning based on the operational plan and execution plan.

5.2.4 **Army.com TD (2005-2007**). This demonstration will focus on providing a seamless, secure, self-organizing, self-healing tactical three-dimensional (3-D) communications backbone capable of bringing web-like Internet capabilities to the individual soldier on the battlefield, currently available only on commercially wired networks. The objective of this effort is to bring this powerful capability to the wireless environment of lower-echelon Army users. The individual soldier will then have a greatly enhanced capacity to perform his mission, allowing him to obtain the information he needs, anytime, untethered to a fixed infrastructure. Army.com focuses on providing moderate-to-high-bandwidth wireless communications to handheld and vehicle-mounted devices to provide internet and intranet services. Commercially developed digital personal communications system (PCS) services, JTRS, and other emerging communications and internet technologies will be leveraged. Secure and nonsecure networks will be connected to provide a secure environment. This capability will be applicable to both command post and dismounted soldier applications. A significant portion of this program will also focus on networking for unmanned aerial vehicles and satellite communications (SATCOM).

5.3 TECHNOLOGY PROGRAMS LEADING TO ENHANCED SURVIVABILITY: COMMUNICATIONS—UNATTENDED SENSOR NETWORKING.

5.3.1 **Smart Sensor Communication Networks (SSCN) TD (2001-2005).** The objective is to develop communications network solutions for forward-deployed, unmanned, clustered entities such as smart munitions, sensors, and robotic systems that will be deployed with the FCS on the digitized battlefield of the future. Sensor technology enables the identification and tracking of enemy movements—critical to survival of a lightweight force. Unfortunately, energy-efficient, networked communications capabilities for miniature microsensors do not exist. The solution will enable adaptive, self-healing, multihop communications networks with optimal routing algorithms that are secure and simultaneously exchange imagery and data traffic among the clustered entities and rearward to all echelons including all those beyond line of sight. Specific technological challenges include the development and adaptation of network protocols, low-cost and low-power radio technologies, high-efficiency, low-profile antennas, near-Earth propagation effect on antennas, and resolution of security issues associated with linking forward unmanned entities with the (secure) tactical internet.

5.4 TECHNOLOGY PROGRAMS LEADING TO ENHANCED SURVIVABILITY: COMMUNICATIONS—INFORMATION ASSURANCE.

5.4.1 **Tactical Command and Control Protect ATD (1998-2002).** This ATD will develop, integrate, validate, and demonstrate hardware and software that protects the systems and networks of the First Digitized Division and FCS from modern network attacks. A security architecture will be developed and demonstrated to provide advanced network access control, intrusion detection and response, malicious code detection and eradication, and security management within tactical communications networks. The ATD leverages existing attack and protects COTS and DoD protection technologies. Field tests and demonstrations will be conducted for RF and wire-based attacks against threat information systems and C2 protect products.

5.4.2 **Tactical Information Assurance Technology TD (2003-2007).** The need to provide adequate information protection for the information systems of the FCS and beyond will continue to be a critical necessity requiring further advances in technology and protection tool development. This program will focus on advancing the state of the art in tactical protect tools and security architecture concepts to enhance the security posture of the digitized force. Advanced security tools that are "network aware" will be pursued at all echelons. System vulnerabilities will be examined based on emerging threats and tools focused in those areas. Advanced tools will be pursued in areas of next-generation intrusion detection sensors, trusted operating systems, tactical biometrics, high-speed tactical guards, computer inoculation, and tactical virtual private networks. Efforts from DARPA, ARL, the Air Force, and the National Security Agency (NSA) in these areas will be leveraged and tailored to tactical needs. Linkages among tools at various echelons will be pursued to provide an information assurance common operational picture for a situational-awareness-type security view.

5.5 TECHNOLOGY PROGRAMS LEADING TO ENHANCED SURVIVABILITY: COMMUNICATIONS—ANTENNAS.

5.5.1 **Antennas for Communication Across the Spectrum TD (1997-2001).** The objective of this demonstration is to develop, leverage, and apply emerging antenna technology to reduce the number of antennas, visual signature (conformal), and cosite and control problems and increase efficiencies and radiation patterns in the 2-MHz – 2- GHz ranges for FCS operations. A second goal is to provide OTM SATCOM antenna capabilities in the X and extremely-high frequency (EHF) bands. Eight different technologies are being explored to address different applications (JTRS, air and ground vehicles, and SATCOM). Wideband technology (30-450 MHz) will be exploited for JTRS application. For air and ground vehicles, structurally embedded reconfigurable antenna technology and structure-tuned antenna/band-switched techniques (225-450 MHz and 30-88 MHz) will be used. SHF and EHF low-profile, self-steering OTM antenna technology will be applied to SATCOM applications. The initial thrust will be to address the broadband requirements for JTRS.

5.5.2 **Advanced Antennas TD (2002-2006).** The objective is to develop a family of highly efficient, practical, cost-effective antennas and subordinate products covering the 30-MHz to 44-GHz frequency range. These antennas will have higher gain and bandwidth to sustain robust, high-data-rate communications, greater agility for OTM operations, and lower profiles for reduced platform visual signatures. They will also be capable of conformal integration within soldiers' clothing for improved mobility and survivability and be functional with the JTRS multiband radio. The body-borne and low-profile antennas will avoid more destructive environmental and ballistic impacts, resulting in substantially reduced attrition rates and logistic burdens.

5.6 TECHNOLOGY PROGRAMS LEADING TO ENHANCED SURVIVABILITY: COMMUNICATIONS—SECURE PERSONAL COMMUNICATIONS.

5.6.1 **Dismounted Warrior Command, Control, Communications, Computers, and Intelligence (C4I) TD (2000-2004).** Advanced C4I technologies emerging from this effort will assist in defining and developing C4I architectures at echelons battalion and below in support of FCS initiatives. Significant military and commercial investments are being exploited in wireless personal communications, mobile computing, and C2 applications to ensure power, weight, and cost objectives are met and that C4I technologies and architectures are optimized for transition through the Land Warrior Modernization Strategy and JTRS Joint Program Office. This will be accomplished through technical collaboration with DARPA, Army Materiel Command Science & Technology (AMC S&T) initiatives identified in the U.S. Army Soldier and Biological Chemical Command Warrior Systems Modernization Strategy, and advanced C4I technologies and architecture designs emerging from the DARPA Small Unit Operations (SUO) Situation Awareness System, GloMo programs, and commercial developers of consumer electronics and wireless communications products.

5.6.2 **Universal Handset TD (2005-2007).** The goal of this program is to develop and demonstrate the ability to have multiple personal communications modes (e.g., terrestrial, satellite, peer to peer, and local loop) in a single handheld device. This will evolve and mature the work begun under the universal handset dual-use science and technology program, which is building proof-of-concept prototypes incorporating peer-to-peer waveforms within a cellular PCS handset. Commercial technology will be leveraged to the maximum extent possible. The concept of the universal handset is to incorporate military-unique features using the commercial cellular handset as the basis. The design of a peer-to-peer capability would allow a single handset to be used at all echelons of the battlefield. This would allow dismounted soldiers to be able to communicate within the team as well as having a reachback into the tactical switched network. All of the above modes will be secured.

5.7 TECHNOLOGY PROGRAMS LEADING TO ENHANCED SURVIVABILITY: COMMUNICATIONS—REACHBACK.

5.7.1 **On-the-Move Tactical Satellite Communications (SATCOM) Technology TD (2000-2004).** The goal is to develop an OTM SATCOM ground terminal capability that can quickly recover from signal blockages due to manmade objects, terrain or groundcover, weather, and other atmospheric effects. These terminals will be used in conjunction with emerging wideband commercial low-earth-orbit, medium-earth-orbit, and military geosynchronous-earth-orbit SATCOM and protected narrowband SATCOM.

5.7.2 **Next Generation Satellite Communications TD (2005-2007).** The objective is to develop a universal, modular, adaptive SATCOM terminal (UMAST) to support the evolving 3-D military global information infrastructure (GII). These terminals will be smaller, lighter, and cheaper than those currently in use. They will be more easily deployable for ground or airborne use and will be fully capable of OTM operation. They will seamlessly interface with terrestrial wired and wireless systems to integrate wide and local area battlefield networks into an intranet providing the warfighter range-independent, secure global connectivity.

5.8 TECHNOLOGY PROGRAMS IN SUPPORT OF FCS AND OBJECTIVE FORCE REQUIREMENTS.

5.8.1 **Dynamic Readdressing and Management for Army 2010 (DRAMA).** This program provides network management products, to include protocols and algorithms, needed to support mobility and allow the network manager the ability to manage over 100 highly mobile nodes.

5.8.2 **Free-Space Optical Communication System (FOCUS).** Focus will develop a new generation of short-range communications. This program will capitalize on the inherent covert attributes of laser and millimeter wave (MMW) communications. The characteristics of extremely narrow beam optical communications systems will be extremely advantageous to achieving the desired covertness. Tracking, signal acquisition/reacquisition, and networking technology will be developed.

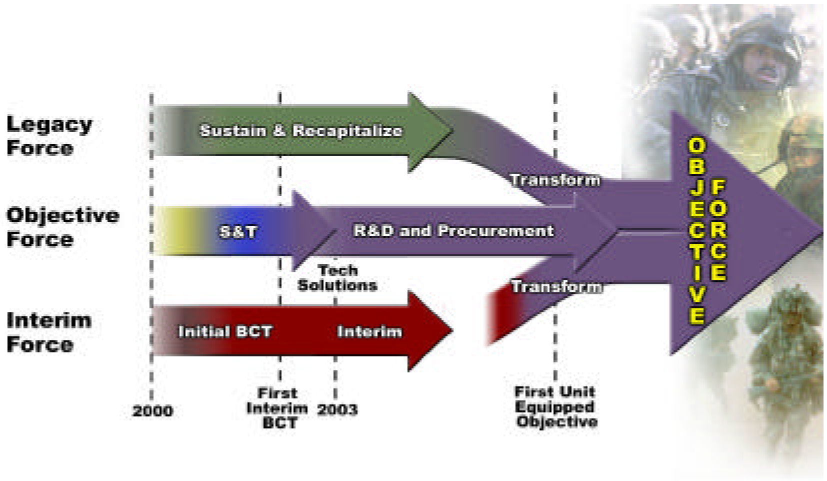
5.8.3 **Information Dissemination Management (IDM)-Tactical.** This program tailors an existing DARPA/Defense Information Systems Agency (DISA) information dissemination management (IDM) tool to meet the Army's tactical needs to intelligently disseminate data directly to the warfighter's ABCS C2 workstation. It provides the tools to dynamically tailor the information system to changing battlefield situations and provides an information manager with functionality that extends the Global Broadcast Service (GBS) to ABCS.

5.8.4 **Smart Networked Radio Technology.** The goal of this program is to combat the lack of frequency spectrum and limited bandwidth by emphasizing what is commonly referred to as "smart networking." This amounts to the judicious use of bandwidth and power while maintaining an efficient data network commensurate with the throughput, delay, and connectivity needs of the users.

5.8.5 **Army Networking Technology.** This program aims to develop the next generation of intelligent, survivable network control technology. It will be consistent with the Smart Networked Radio Technology Program by providing network control and management based on a model of the human thought process as well as more traditional computation models.

6. SUMMARY

6.0 GENERAL. C4 is an essential element to success in meeting the requirements of the Army's Transformation Campaign as shown in Figure 6.0-1. In particular, the FCS concept hinges on providing secure, dependable, and adaptable C4 across all spectrums of conflict anywhere in the world where U.S. forces might be employed.



. . . Responsive, Deployable, Agile, Versatile, Lethal, Survivable, Sustainable.

Figure 6.0-1. Army Transformation Campaign Strategy

6.0.1 **<u>The Information Technology Opportunity</u>.** The explosion of information technologies presents a unique opportunity to exploit their potential for increasing combat capabilities. The digitization of the battlefield efforts holds great promise for significantly enhancing combat power and survivability of Army forces in combat. Care, however, must be exercised to ensure that a balanced C4 enhancement program is implemented that does not assume or "wish away" problems or shortfalls. Distributed databases, no matter how survivable or how much "good" information they contain, are of no use if a transport mechanism is not in place to move this information around the battlefield. No sophisticated processing of information is useful if it can't be displayed in a timely and comprehensible manner. Solving the complex problem of digitizing the battlefield is certainly achievable, but not easy and without cost. The efforts in developing ATCCS, Enhanced Position Location Reporting System (EPLRS), and Joint Tactical Information Distribution System (JTIDS) clearly demonstrate the complexities and costs associated with fielding integrated C4 systems. It is one thing to demonstrate a capability using COTS technology, but it is often a totally different thing to convert that demonstrated capability into a survivable, integrated system.

6.0.2 **<u>Technology Advances</u>.** Advances in microelectronics, photonics, and acoustics will increase operational bandwidth, enhance data and real-time signal processing, and dramatically increase analysis capabilities. To get information down to the soldier level, the size of C4 devices and systems will have to be much smaller, and the scaling down of Very High-Speed Integrated Circuit (VHSIC) has limits. Compound semiconductor technology, monolithic structures, quantum electronic devices, superlattice materials, and opto-electronic integration hold great promise. Photonic devices being developed will allow the transmission and processing of information at the speed of light. Advances in the integration of technologies to counter CNAs are required to provide a secure architecture that provides advanced network access control, intrusion detection, and response mechanisms within tactical communications networks to dramatically increase the probability of continued operations in an offensive IO environment.

6.1 ROADMAPS TO C4 MODERNIZATION. Improvements across all C4 areas must be introduced in a coordinated and simultaneous manner if goals are to be met. Figure 6.1-1 displays the current road map to C4 modernization. □□

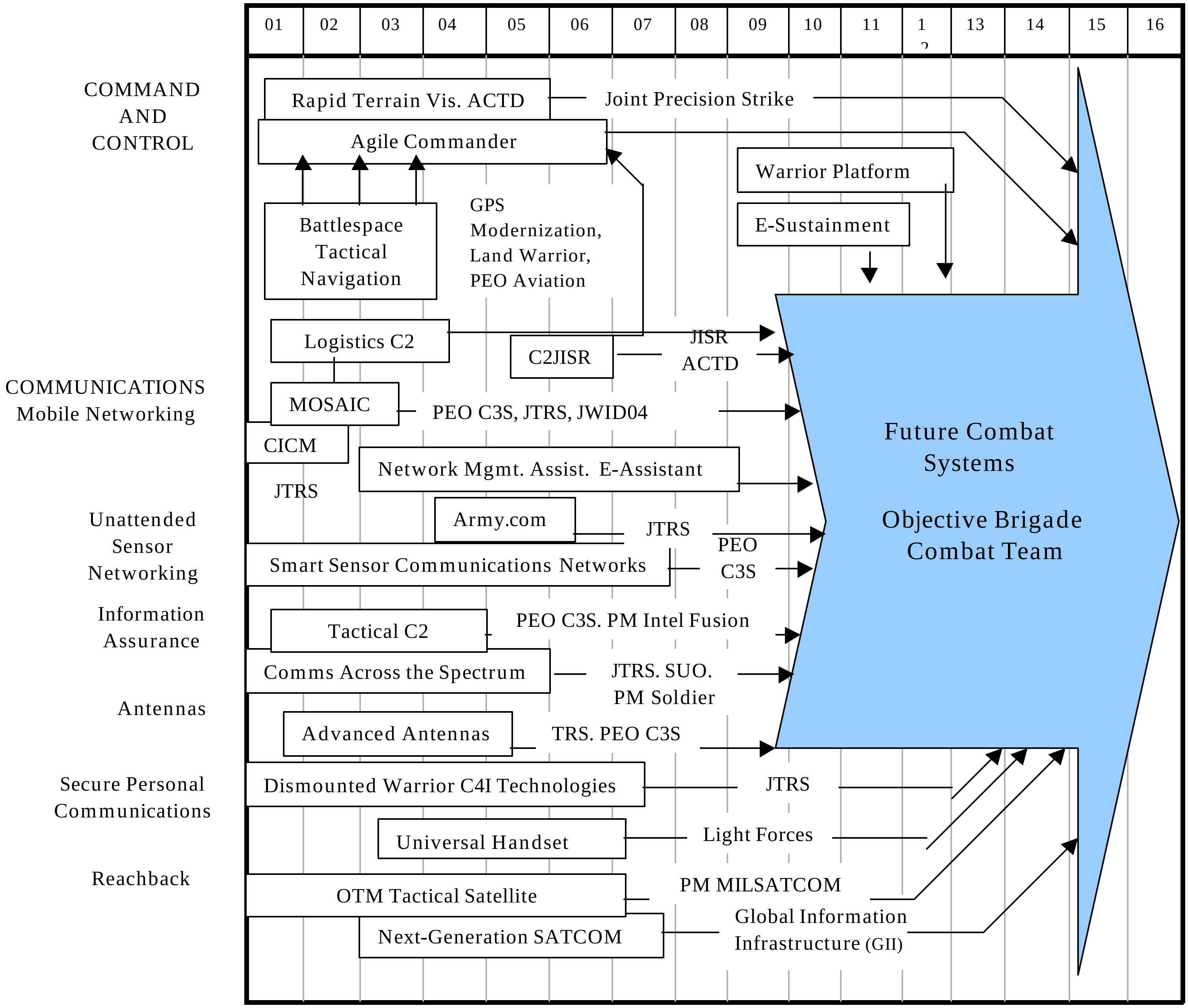


Figure 6.1-1 C4 Modernization Roadmap

6.2 C4 CONTRIBUTION TO FORCE SURVIVABILITY. C4 systems enhance the survivability of the force by being able to avoid detection, operate in an EW and NBC environment, provide information to enhance awareness of vulnerabilities, and protect information from compromise. Survivability can be enhanced by improving performance in eight basic areas (Figure 6.2-1).

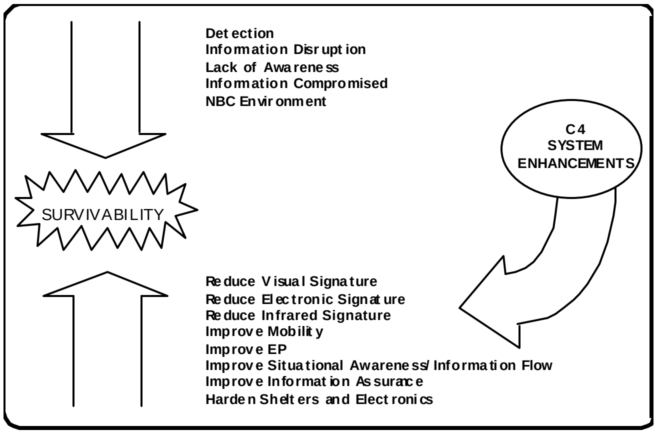


Figure 6.2-1. C4 Survivability Enhancement Areas

6.3 SURVIVABILITY ENHANCEMENT RECOMMENDATIONS. The following survivability enhancement recommendations are presented as a focus for requirements developers and technology base researchers. They suggest ways to reduce existing and currently projected survivability shortfalls.

- C4 systems survivability is of no consequence if the information they carry is corrupted. Improvements in information assurance should be made as soon as possible. Continue to develop MLS to make the flow of information envisioned by the digitization initiatives a reality. Ensure MLS is developed for both the information transport and information management systems. As expert systems and artificial intelligence systems are developed, they will play a key role in expanding MLS. Use “trusted guards” to employ these technologies to permit sanitization, downgrading, and release of classified information when required. Consider physical access controls using biometric characteristics, such as retina patterns, fingerprints, palm prints, and finger measurements, to authenticate the access to highly classified or restricted data.

- Continue to develop systems and capabilities to allow dispersion of CP elements that can provide for fast installation, large capacity, low signature, and reduced manpower.

- Develop capabilities for sharing antennas, conformal antennas, remote antennas, and steerable directional antennas.

- Reduce power consumption of radio systems and automated C2 systems, thus reducing the power requirements of a CP. Improve power generation equipment to provide reliable power with a reduced thermal and aural signature.

- Armored CP vehicles with installed C4 systems are needed to enhance the mobility of the commander. Mobile CPs must be capable of providing the same information to the commander that is available in a fixed CP. Systems are needed that share information across all functional areas at all echelons. Information provided by these systems must be based on common data residing on dispersed databases. Systems must be easy to operate and capable of providing the information when, where, and in whatever form is required by the user. Decision aids, expert systems, and artificial systems must be used to assist in decision processes.

- Extend the range of the MSE nodes to allow the robust network to be configured over vast distances. Develop better frequency and key management systems with artificial intelligence (AI) and expert systems capabilities. Enhance LOS radio capability.
- Develop technologies that will allow communications between widely dispersed elements of the CP. Systems must produce no unique signatures, be quickly and easily installed, and be capable of carrying a large volume of data.
- Develop mobile satellite antennas that can support OTM satellite communications in the EHF range.
- It is critical to overall survivability that networks have the capability to transport increasing amounts of information accurately, securely, and with built-in redundancy. Currently, networks lag communications system development. Data distribution continues to be a concern. Planned demonstrations, if successful, should go a long way toward resolving data distribution on the battlefield.
- Increase the survivability of communications over extended ranges. Satellites, satellite clones, manned and unmanned aerial vehicles, and HF radios are potential technologies to be further exploited.
- Upgrade Defense Satellite Communication System (DSCS) to enhance its ability to survive in a jamming environment and, for some applications, in a nuclear environment. Additionally, develop systems that enhance the management and reconfiguring of the satellite and its ground stations.
- Develop an acquisition strategy to integrate COTS/Government off-the-shelf (GOTS) tools to counter CNAs.
- Develop a strategy for managing information protection tools.

6.4 CONCLUSIONS. While C4 is a key to the survivability of forces deployed in a combat zone, it can also be a detriment to survivability through its electronic, visual, and IR signatures. Technologies and systems that reduce the signature of CPs and communications facilities, provide a common signal footprint for all forces, facilitate dispersal, and allow full C2 operations on the move are needed. Likewise, systems that can move to the rear or out of the forward combat zone (e.g., communications nodes and data-processing capabilities) and still provide support will increase survivability. Systems are essential that provide a multitude of communications paths capable of dynamic reconfiguration and can respond to nodal or path losses with no degradation of information being provided to the combatants.

- The EA threat will cause next-generation C4 systems to rely heavily on integrated EP imbedded in terminals, networks, and links. Features that will be considered in order to negate the impact of the EA threat include (1) maintenance of a uniform RF signature over the battlefield in order to deny identification of communication centers, CPs, and weapons systems; (2) RF emitters that are difficult to intercept; (3) communication wave forms that are difficult to jam; (4) extensive use of MLS; (5) redundant and coupled networks, databases, and processors; and (6) enhanced mobility for communications while OTM.

- Improved situational awareness and expanded, shared information are critical to survivability on the battlefields of the future. Also needed are systems and technologies that can contribute to increased processing, correlation and display of information, and uninterrupted transmission to all parts of the battlefield. The fast-paced digitized battlefield will require systems that assist the warfighter in making key decisions. To process information will require increased computational capabilities starting with ruggedized hardware (e.g., drives that operate on the move), fault-tolerant hardware and software, neural networks, fuzzy logic, parallel processing, and high-speed logic. Artificial intelligence, expert systems, decision theory, parallel and distributed processing, distributed databases, and information fusion must be incorporated in future C4 systems whenever they can make a measurable contribution to improving the ability to command and control the future battlefield.

- The reduced threat of nuclear war has reduced emphasis on hardening of electronic systems. This makes systems in general more vulnerable to the effects of direct, indirect fire and the EM range of threats. The use of COTS equipment is cost effective and allows introduction of improved technologies into the field more quickly. The tradeoff is equipment that is less rugged and less survivable.

- The increased reliance on information systems makes information assurance a prime consideration when identifying survivability shortfalls. The hardware may survive, but the system could become useless if the data is corrupted or destroyed. The threat from CNAs is real and must be addressed. Future systems are integrating security measures (e.g., firewalls), but the fix is only short term if there is not a continuous process to update the security measures to account for new technologies. Combining the efforts in the development of new technologies with the implementation of the “Defense in Depth” and the execution of “Red Teaming” will go a long way in achieving information assurance. Three primary information security measures that must be continuously reviewed are as follows:

1) procedures for quality assurance,

2) identification/denial of CNAs, and

3) hardening of computer systems.

Quality-assurance procedures include configuration control and reduction of inadvertent corruption of both data and processes. In order to protect automated C4 systems, the first step is to understand the threat (section 3). From the standpoint of information assurance, protection against intrusion into friendly computer networks is accomplished through denying unauthorized entry. The vast percentage of intrusions result from human error. Training and operations security (OPSEC) compliance by system managers, operators, and users are the best measures to combat system compromises. In addition, system administrators must be able to track down intruders. In addition, system programs should be hardened against intruders' attempts to gain vital information or damage information flow. No protection plan is perfect, and protection/restoration resources are finite. Operation plans (OPLAN) and operation orders (OPORD) specify the priorities of protection efforts. The bottom line is that while technology will enhance the survivability of the C4 systems, system operators play a critical role in system survivability.

- Another concern arising from enhanced situational awareness is co-site interference. Research and technology demonstrations are ongoing and must lead to solutions that can be implemented in the field. Very similar to the problems encountered when SINCGARs interfere, the expanded use of the EM spectrum will create serious problems unless managed properly. Indirectly, this affects the survivability of systems and personnel. The increased reliance on C4 systems makes it even more critical that systems are functioning properly and without interference. Whether caused by friendly or threat forces, interference impedes the ability of the commander to maximize the potential of fielded technologies.

Survivability improvements do not just happen. They come about through a rigorous process of analysis, research, simulation, modeling, and testing to identify areas where survivability gains can and are being achieved. Survivability must be built into a program and considered during all stages of its development. It is imperative to determine critical survivability issues and expend the necessary resources to perform analysis and experimentation to resolve these issues. An analysis of the survivability of C4 systems clearly provides the understanding of the direction required to improve the probability of success on the battlefield. The technologies to support the warfighter are becoming available, but if there is not a thorough understanding of the shortfalls, the Army remains at a distinct disadvantage. C4 technology advancements to support the warfighter must be closely scrutinized to ensure that the benefits are weighed against the costs associated with increased susceptibility to unauthorized access.

LIST OF ACRONYMS AND ABBREVIATIONS

3-D	Three-Dimensional
ABCS	Army Battle Command System
ACAS	Antenna Communications Across the Spectrum
ACTD	Advanced Concept Technology Demonstration
AI	Artificial Intelligence
AR	Army Regulation
ARL	Army Research Laboratory
ARM	Anti-Radiation Missile
ATCCS	Army Tactical Command and Control System
ATD	Advanced Technology Demonstration
BCT	Brigade Combat Team
BFA	Battlefield Functional Area
BTN	Battlespace Tactical Navigation
BW	Biological Weapons
C2	Command and Control
C2JISR	Command and Control for Joint Intelligence, Surveillance, and Reconnaissance
C4	Command, Control, Communications, and Computers
C4I	Command, Control, Communications, Computers, and Intelligence
CAS	Close Air Support
CB	Chemical and Biological
CICM	Communications Integration and Cosite Mitigation
CM	Cruise Missile, Countermeasure
CNA	Computer Network Attack
COA	Course of Action
COMSEC	Communications Security
COTS	Commercial-Off-The-Shelf
CP	Command Post
DARPA	Defense Advanced Research Projects Agency
DEW	Directed Energy Weapon
DF	Direction Finding
DISA	Defense Information Systems Agency
DOCC	Deep Operations Coordination Center
DoD	Department of Defense
DPICM	Dual-Purpose Improved Conventional Munition
DRAMA	Dynamic Readressing and Management for Army
DSCS	Defense Satellite Communication System
EA	Electronic Attack
ECM	Electronic Countermeasures
EDOCC	Enhanced Deep Operations Coordination Center
EHF	Extremely High Frequency

EM	Electromagnetic
EMP	Electromagnetic Pulse
EP	Electronic Protection
EPLRS	Enhanced Position Location Reporting System
ES	Electronic Warfare Support
EW	Electronic Warfare

FBCB2	Force XXI Battle Command for Brigade and Below
FCS	Future Combat System
FEC	Forward Error Correction
FLOT	Forward Line of Troops
FOCUS	Free-Space Optical Communication System
FTP	File Transfer Protocol
FY	Fiscal Year

GBS	Global Broadcast System
GCCS-A	Global Command and Control System - Army
GIE	Global Information Environment
GII	Global Information Infrastructure
GloMo	Global Mobile
GOTS	Government Off-The-Shelf
GPS	Global Positioning System

HF	High Frequency
HPM	High-Power Microwave

IA	Information Assurance
ICM	Improved Conventional Munitions
ICMP	Internet Control Message Protocol
IDM	Information Dissemination Management
IO	Information Operations
IP	Internet Protocol
IR	Infrared
ISR	Intelligence, Surveillance, and Reconnaissance
ISS	Information Security System

JFLCC	Joint Land Force Component Commander
JTIDS	Joint Tactical Information Distribution System
JTRS	Joint Tactical Radio System

LAN	Local Area Network
LOS	Line-of- Sight
LPD	Low Probability-of-Detection
LW	Land Warrior

M&S	Modeling and Simulation
MAIS	Major Automated Information System
MANPRINT	Manpower and Personnel Integration
MDAPS	Mandatory Procedures for Major Defense Acquisition Programs
MIE	Military Information Environment

MMW	Millimeter Wave
MOSAIC	Multifunction On-the-Move Secure, Adaptive, Integrated Communications
MOUT	Military Operations on Urbanized Terrain
MSE	Mobile Subscriber Equipment
NBC	Nuclear, Biological, and Chemical
NFS	Network File System
NIS	Network Information System
NSA	National Security Agency
OCR	Optical Character Reader
OPORD	Operations Order
OPLAN	Operations Plan
OPSEC	Operational Security
OSPF	Open Shortest Path First
OTM	On-the-Move
PCS	Personal Communications System
QOS	Quality of Service
RF	Radio Frequency
RTV	Rapid Terrain Visualization
SA	Situational Awareness
SATCOM	Satellite Communications
SHF	Super High Frequency
SINCGARS	Single-Channel Ground and Airborne Radio System
SLAD	Survivability/Lethality Analysis Directorate
SMTP	Simple Mail Transfer Protocol
SNMP	Simple Network Management Protocol
SOF	Special Operations Forces
SSCN	Smart Sensor Communications Network
SUID	Superuser Identification
SUO	Small Unit Operations
TBM	Tactical Ballistic Missile
TACACS	Terminal Access Controller Access Control System
TD	Technology Demonstration
TFTP	Trivial File Transfer Protocol
TI	Tactical Internet
TTY	Teletypewriter
UHF	Ultra High Frequency
UID	User Identifier
UMAST	Universal, Modular, Adaptive SATCOM Terminal
UUDECODE	User-to-User Decode
VHF	Very High Frequency
VHSIC	Very High Speed Integrated Circuit

WAN	Wide Area Network